MINISTERIO DE EDUCACIÓN

LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
PRIMERA CONVOCATORIA

BASES

CONTRATACIÓN DE BIENES

"ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACIÓN"

2011

MINISTERIO DE EDUCACION

Avenida De la Poesía 155. Altura de la cdra. 19. Av. Javier Prado Este-San Borja Lima

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCESO DE SELECCIÓN

(ESTA SECCIÓN NO PUEDE MODIFICARSE EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD, SALVO AQUELLAS DISPOSICIONES QUE EXPRESAMENTE SE INDIQUE EN LAS BASES QUE PUEDEN SER INCLUIDAS Y/U OMITIDAS)

CAPÍTULO I

ETAPAS DEL PROCESO DE SELECCIÓN

1.1 CONVOCATORIA

Se efectuará de conformidad con lo señalado en el Artículo 51º del Reglamento, en la fecha señalada en el cronograma.

1.2 BASE LEGAL

- Ley Nº 28411, Ley General del Sistema Nacional del Presupuesto.
- Decreto Legislativo Nº 1017, que aprueba la Ley de Contrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 184-2008-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo N° 021-2009-EF – Modificación del Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo N° 140-2009-EF – Modificación del Reglamento de la Ley de Contrataciones del Estado.
- Directivas de OSCE
- Ley Nº 27444, Ley del Procedimiento Administrativo General.
- Código Civil.
- Ley Nº 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Decreto Supremo Nº 007-2008-TR, Texto Único Ordenado de la Ley de Promoción de la Competitividad, Formalización y Desarrollo de la Micro y Pequeña y del acceso al empleo decente, Ley MYPE.
- Decreto Supremo Nº 008-2008-TR, Reglamento de la Ley MYPE.

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

Para la aplicación del derecho deberá considerarse la especialidad de las normas previstas en las presentes Bases.

1.3 REGISTRO DE PARTICIPANTES Y ENTREGA DE BASES

El registro de participantes se efectuará desde el día siguiente de la convocatoria y hasta un (01) día hábil después de haber quedado integradas las Bases. En el caso de propuestas presentadas por un consorcio, bastará que se registre uno de sus integrantes, de conformidad con el Artículo 53º del Reglamento.

La persona natural o persona jurídica que desee participar en el proceso de selección deberá acreditar estar con inscripción vigente en el Registro Nacional de Proveedores (RNP) conforme al objeto contractual. La Entidad verificará la vigencia de la inscripción en el RNP y que no se encuentra inhabilitado para contratar con el Estado.

MUY IMPORTANTE:
Para participar de un proceso de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores se encuentren inscritos, en el registro correspondiente, ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, podrá ingresarse a la siguiente dirección electrónica: www.rnp.gob.pe.

Al registrarse, el participante deberá señalar la siguiente información: Nombres y apellidos (persona natural), DNI, razón social (persona jurídica), número de RUC, domicilio legal, teléfono**.**

De acuerdo con lo establecido en el artículo 52º del Reglamento, la persona natural o jurídica que desee ser notificada electrónicamente, deberá consignar una dirección de correo electrónico y mantenerla activa, a efecto de las notificaciones que, conforme a lo previsto en el Reglamento, deban realizarse. La notificación a través del SEACE prevalece sobre cualquier medio que se haya utilizado adicionalmente, siendo responsabilidad del participante el permanente seguimiento del respectivo proceso a través del SEACE.

1.4 FORMULACIÓN DE CONSULTAS A LAS BASES

Las consultas a las Bases serán presentadas por un periodo mínimo de cinco (05) días hábiles, contados desde el día siguiente de la convocatoria, de conformidad con lo establecido en el artículo 55º del Reglamento.

1.5 ABSOLUCIÓN DE CONSULTAS A LAS BASES

La decisión que tome el Comité Especial con relación a las consultas presentadas constará en el pliego absolutorio que se notificará a través del SEACE y a los correos electrónicos de los participantes que así lo hubieran solicitado, de conformidad con lo establecido en el Artículo 55º del Reglamento, en la fecha señalada en el cronograma del proceso de selección.

El plazo para la absolución no podrá exceder de cinco (5) días hábiles contados desde el vencimiento del plazo para recibir consultas.

La absolución de consultas que se formulen al contenido de las Bases, se considerarán como parte integrante de ésta y del Contrato.

MUY IMPORTANTE:
No se absolverán consultas a las Bases que se presenten extemporáneamente o que sean formuladas por quienes no se han registrado como participantes.

1.6 FORMULACIÓN DE OBSERVACIONES A LAS BASES

Las observaciones a las Bases serán presentadas dentro de los cinco (05) días hábiles siguientes de haber finalizado el término para la absolución de las consultas, de conformidad con lo establecido en el artículo 57º del Reglamento.

1.7 ABSOLUCIÓN DE OBSERVACIONES A LAS BASES

El Comité Especial notificará la absolución de las observaciones a través del SEACE y a los correos electrónicos de los participantes que así lo hubieran solicitado, de conformidad con lo establecido en el Artículo 57º del Reglamento, en la fecha señalada en el cronograma del proceso de selección.

El plazo para la absolución no debe exceder de los cinco (5) días hábiles desde el vencimiento del plazo para recibir observaciones.

La absolución de las observaciones se considerará como parte integrante de las Bases y del Contrato.

MUY IMPORTANTE:
No se absolverán observaciones a las Bases que se presenten extemporáneamente o que sean formuladas por quienes no se han registrado como participantes.

1.8 ELEVACIÓN DE OBSERVACIONES A LA ENTIDAD

El plazo para solicitar la elevación de observaciones al Titular de la Entidad es de tres (3) días hábiles, computados desde el día siguiente de la notificación del pliego absolutorio a través del SEACE. Dicha opción no sólo se originará cuando las observaciones formuladas no sean acogidas por el Comité Especial, sino, además, cuando el observante considere que el acogimiento declarado por el Comité Especial continúa siendo contrario a lo dispuesto por el artículo 26° de la Ley, cualquier otra disposición de la normativa sobre contrataciones del Estado u otras normas complementarias o conexas que tengan relación con el proceso de selección.

Igualmente, cualquier otro participante que se hubiere registrado como tal antes del vencimiento del plazo previsto para formular observaciones, tendrá la opción de solicitar la elevación de las Bases, cuando habiendo sido acogidas las observaciones formuladas por los observantes, considere que la decisión adoptada por el Comité Especial es contraria a lo dispuesto por el artículo 26° de la Ley, cualquier otra disposición de la normativa sobre contrataciones del Estado u otras normas complementarias o conexas que tengan relación con el proceso de selección.

El plazo que tiene el Titular de la Entidad para emitir y notificar el Pronunciamiento a través del SEACE será no mayor de ocho (8) días hábiles. Este plazo es improrrogable y será contado desde la presentación de la solicitud de elevación de las Bases.

La competencia del Titular de la Entidad para emitir el Pronunciamiento es indelegable".

1.9 INTEGRACIÓN DE LAS BASES

El Comité Especial integrará las Bases como reglas definitivas del presente proceso de selección, una vez absueltas todas las consultas y/u observaciones o si éstas no se han presentado, no pudiendo ser cuestionadas en ninguna otra vía ni modificadas por autoridad administrativa alguna, bajo responsabilidad del Titular de la Entidad. Esta restricción no afecta la competencia del Tribunal para declarar la nulidad del proceso por deficiencias en las Bases.

Las Bases Integradas, de ser el caso, deberán contener los cambios producidos como consecuencia de las consultas y observaciones formuladas y aceptadas o acogidas por el Comité Especial, y/o de lo dispuesto en el Pronunciamiento emitido por el Titular de la Entidad o por el OSCE, de ser el caso.

Corresponde al Comité Especial, bajo responsabilidad, integrar las Bases y publicarlas en el SEACE, conforme lo establecen los Artículos 59º y 60º del Reglamento.

De conformidad con el artículo 31º del Reglamento, el Comité Especial no podrá efectuar modificaciones de oficio al contenido de las Bases, bajo responsabilidad.

1.10 FORMA DE PRESENTACIÓN Y ALCANCES DE LAS PROPUESTAS

Todos los documentos que contengan información referida a los requisitos para la admisión de propuestas y factores de evaluación se presentarán en idioma castellano o, en su defecto, acompañados de traducción efectuada por traductor público juramentado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que podrá ser presentada en el idioma original. El postor será responsable de la exactitud y veracidad de dichos documentos. La omisión de la presentación del documento o su traducción no es subsanable.

Las propuestas se presentarán en dos (2) sobres cerrados, de los cuales el primero contendrá la propuesta técnica y el segundo la propuesta económica.

Si las propuestas se presenten en hojas simples se redactarán por medios mecánicos o electrónicos, llevarán el sello y la rúbrica del postor y serán foliadas correlativamente empezando por el número uno.

Asimismo, cuando las propuestas tengan que ser presentadas total o parcialmente mediante formularios o formatos, éstos podrán ser llenados por cualquier medio, incluyendo el manual, debiendo llevar el sello y la rúbrica del postor o su representante legal o mandatario designado para dicho fin.

Las personas naturales podrán concurrir personalmente o a través de su apoderado debidamente acreditado ante el Comité Especial, mediante carta poder simple **(Formato N° 01).** Las personas jurídicas lo harán por medio de su representante legal acreditado con copia simple del documento registral vigente que consigne dicho cargo o a través de su apoderado acreditado con carta poder simple suscrita por el representante legal, a la que se adjuntará el documento registral vigente que consigne la designación del representante legal **(Formato Nº 01)**.

1.11 PRESENTACIÓN DE PROPUESTAS

La presentación de propuestas se realiza en acto público, en la fecha y hora señaladas en el calendario del proceso.

El acto se inicia cuando el Comité Especial empieza a llamar a los participantes en el orden en que se registraron para participar en el proceso, para que entreguen sus propuestas. Si al momento de ser llamado el participante no se encuentra presente, se le tendrá por desistido. Si algún participante es omitido, podrá acreditarse con la presentación de la constancia de su registro como participante.

Los integrantes de un consorcio no podrán presentar propuestas individuales ni conformar más de un consorcio.

"Los integrantes de un consorcio no podrán presentar propuestas individuales ni conformar más de un consorcio en un mismo ítem, lo que no impide que puedan presentarse individualmente o conformando otro consorcio en ítems distintos"[1].

Después de recibidas las propuestas, el Comité Especial procederá a abrir los sobres que contienen la propuesta técnica de cada postor.

El Comité Especial comprobará que los documentos presentados por cada postor sean los solicitados por las Bases, la Ley y el Reglamento. De no ser así, devolverá la propuesta, teniéndola por no presentada, salvo que el postor exprese su disconformidad, en cuyo caso se anotará tal circunstancia en el acta y el Notario (o Juez de Paz) mantendrá la propuesta en su poder hasta el momento en que el postor formule apelación. Si se formula apelación se estará a lo que finalmente se resuelva al respecto.

De presentarse situaciones de subsanación de la propuesta técnica, se procederá de acuerdo al Artículo 68° del Reglamento.

Después de abierto cada sobre que contiene la propuesta técnica, el Notario (o Juez de Paz) procederá a sellar y firmar cada hoja de los documentos de la propuesta técnica. A su vez, si las Bases han previsto que la evaluación y calificación de las propuestas técnicas se realice en fecha posterior, el Notario (o Juez de Paz) procederá a colocar los sobres cerrados que contienen las propuestas económicas dentro de uno o más sobres, los que serán debidamente sellados y firmados por él, por los miembros del

[1] Esta disposición sólo deberá ser adicionada cuando se convoque el proceso de selección según relación de ítems.

Comité Especial y por los postores que así lo deseen, conservándolos hasta la fecha en que el Comité Especial, en acto público, comunique verbalmente a los postores el resultado de la evaluación de las propuestas técnicas.

Al terminar el acto público, se levantará un acta, la cual será suscrita por el Notario (o Juez de Paz), por todos sus miembros, así como por los veedores y los postores que lo deseen.[2]

1.12 CONTENIDO DE LA PROPUESTA ECONÓMICA

La propuesta económica (Sobre Nº 2) deberá incluir obligatoriamente lo siguiente:

a) La oferta económica, en nuevos soles[3], incluidos todos los tributos, seguros, transportes, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien a contratar; excepto la de aquellos postores que gocen de exoneraciones legales. La Entidad no reconocerá pago adicional de ninguna naturaleza.

El monto total de la propuesta económica y los subtotales que lo componen deberán ser expresados con dos decimales. Los precios unitarios podrán ser expresados con más de dos decimales.

a) Garantía de seriedad de oferta[4]

"Tratándose de un proceso según relación de ítems, cuando los postores se presenten a más de un ítem, deberán presentar sus propuestas económicas en forma independiente[5]".

1.13 EVALUACIÓN DE PROPUESTAS

La evaluación de propuestas se realizará en dos (02) etapas: La evaluación técnica y la evaluación económica.

Los máximos puntajes asignados a las propuestas son las siguientes:
Propuesta Técnica : 100 puntos
Propuesta Económica : 100 puntos

1.13.1 Evaluación Técnica

Se verificará que la propuesta técnica contenga los documentos de presentación obligatoria y cumpla con los requerimientos técnicos mínimos contenidos en las presentes Bases. Las propuestas que no cumplan dichos requerimientos no serán admitidas.

---

[2] Deberá tenerse en cuenta que, de conformidad con lo dispuesto en el artículo 64º del Reglamento, en los actos de presentación de propuestas y otorgamiento de la buena pro se podrá contar con la presencia de un representante del Sistema Nacional de Control, quien participará como veedor y deberá suscribir el acta correspondiente. Asimismo, la inasistencia de dicho representante no viciará el proceso.

[3] En cada caso concreto deberá consignarse la moneda que resulte aplicable.

[4] En caso de convocarse a un proceso de selección según relación de ítems, cuando el valor referencial del ítem corresponda a una Adjudicación de Menor Cuantía, bastará que el postor presente en su propuesta técnica una declaración jurada donde se comprometa a mantener vigente su oferta hasta la suscripción del contrato.

[5] Luego de efectuada la evaluación técnica, cabe la posibilidad que dicho postor haya obtenido el puntaje necesario para acceder a la evaluación económica únicamente en algunos de los ítems a los que se presentó, por lo que, de acuerdo con el artículo 71º del Reglamento, correspondería devolver las propuestas económicas sin abrir, lo que no resultaría posible si la totalidad de las propuestas económicas del postor se incluyen en un solo sobre. Por tanto, resulta necesario precisar este aspecto.

Sólo a aquellas propuestas admitidas, el Comité Especial les aplicará los factores de evaluación previstos en las Bases y asignará los puntajes correspondientes, conforme a los criterios establecidos para cada factor.

Las propuestas técnicas que no alcancen el puntaje mínimo de sesenta (60) puntos, serán descalificadas en esta etapa y no accederán a la evaluación económica.

1.13.2 Evaluación Económica

Si la propuesta económica excede el valor referencial, será devuelta por el Comité Especial y se tendrá por no presentada, conforme lo establece el artículo 33º de la Ley.

La evaluación económica consistirá en asignar el puntaje máximo establecido a la propuesta económica de menor monto. Al resto de propuestas se les asignará puntaje inversamente proporcional, según la siguiente fórmula:

$$Pi = \frac{Om \times PMPE}{Oi}$$

Donde:

i = Propuesta
Pi = Puntaje de la propuesta económica i
Oi = Propuesta Económica i
Om = Propuesta Económica de monto o precio más bajo
PMPE = Puntaje Máximo de la Propuesta Económica

1.14 ACTO PÚBLICO DE OTORGAMIENTO DE LA BUENA PRO

En la fecha señalada en las Bases, el Comité Especial procederá a otorgar la Buena Pro a la propuesta ganadora, dando a conocer los resultados del proceso de selección a través de un cuadro comparativo en el que se consignará el orden de prelación y el puntaje técnico, económico y total obtenidos por cada uno de los postores.

La evaluación de las propuestas económicas se realizará de conformidad con el procedimiento establecido en las presentes Bases.

La determinación del puntaje total se hará de conformidad con el artículo 71º del Reglamento.

El Presidente del Comité Especial anunciará la propuesta ganadora indicando el orden en que han quedado calificados los postores a través del cuadro comparativo.

En el supuesto que dos (02) o más propuestas empatasen, el otorgamiento de la Buena Pro se efectuará observando lo señalado en el Artículo 73º del Reglamento.

Al terminar el acto público se levantará un acta, la cual será suscrita por el Notario (o juez de paz), por todos los miembros del Comité Especial y por los postores que deseen hacerlo.

El otorgamiento de la Buena Pro, se presumirá notificado a todos los postores en la misma fecha, oportunidad en la que se entregará a los postores copia del acta de otorgamiento de la buena pro y el cuadro comparativo, detallando los resultados en cada factor de evaluación. Dicha presunción no admite prueba en contrario.

Esta información se publicará el mismo día en el SEACE.

1.15 CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más propuestas, el consentimiento de la Buena Pro se producirá a los ocho (8) días hábiles de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

En el caso que se haya presentado una sola oferta, el consentimiento de la Buena Pro se producirá el mismo día de la notificación de su otorgamiento.

El consentimiento de la Buena Pro se publicará en el SEACE al día siguiente de haber quedado consentido el otorgamiento de la buena pro.

1.16 CONSTANCIA DE NO ESTAR INHABILITADO PARA CONTRATAR CON EL ESTADO

De acuerdo con el artículo 282º del Reglamento, a partir del día hábil siguiente de haber quedado consentida la Buena Pro hasta el décimo quinto día hábil de producido tal hecho, el postor ganador de la Buena Pro debe solicitar ante el OSCE la expedición de la constancia de no estar inhabilitado para contratar con el Estado.

El OSCE no expedirá constancias solicitadas fuera del plazo indicado.

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCESO DE SELECCIÓN

2.1 Recurso de apelación

A través del recurso de apelación se impugnan los actos dictados durante el desarrollo del proceso de selección, desde la convocatoria hasta aquellos emitidos antes de la celebración del contrato.

El recurso de apelación se presentará ante la Entidad que convocó el proceso de selección que se impugna, y será conocido y resuelto por el Titular de la Entidad

El Tribunal será competente para conocer y resolver las controversias que surjan en los procesos de selección de las contrataciones que se encuentren bajo los alcances de tratados o acuerdos internacionales donde se asuman compromisos en materia de contratación pública.

2.2 Plazos de interposición del recurso de apelación

La apelación contra el otorgamiento de la Buena Pro o contra los actos dictados con anterioridad a ella debe interponerse dentro de los ocho (8) días hábiles siguientes de haberse otorgado la Buena Pro.

La apelación contra los actos distintos a los indicados en el párrafo anterior debe interponerse dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III

SUSCRIPCIÓN DEL CONTRATO

3.1 DE LOS CONTRATOS

Una vez que quede consentido o administrativamente firme el otorgamiento de la Buena Pro, la Entidad deberá, dentro del plazo de dos (2) días hábiles siguientes al consentimiento de la Buena Pro, citar al postor ganador otorgándole el plazo establecido en las Bases, el cual no podrá ser menor de cinco (5) ni mayor de diez (10) días hábiles, dentro del cual deberá presentarse a la sede de la Entidad para suscribir el contrato con toda la documentación requerida. En el supuesto que el postor ganador no se presente dentro del plazo otorgado, se procederá de acuerdo a lo dispuesto en el artículo 148° del Reglamento.

El contrato será suscrito por la Entidad, a través del funcionario competente o debidamente autorizado, y por el ganador de la Buena Pro, ya sea directamente o por medio de su apoderado, tratándose de persona natural, y tratándose de persona jurídica, a través de su representante legal, de conformidad con lo establecido en el Artículo 139° del Reglamento.

Para suscribir el contrato, el postor ganador de la Buena Pro deberá presentar, además de los documentos previstos en las Bases, los siguientes:

- Constancia vigente de no estar inhabilitado para contratar con el Estado.
- Garantía de fiel cumplimiento y por el monto diferencial de la propuesta, de ser el caso, cuya vigencia se extiende hasta la conformidad de la recepción de la prestación a cargo del contratista, salvo casos de excepción;
- Contrato de consorcio con firmas legalizadas de los asociados, de ser el caso.

3.2 VIGENCIA DEL CONTRATO

En aplicación de lo dispuesto en el artículo 149º del Reglamento, el contrato tiene vigencia desde el día siguiente de la suscripción del documento que lo contiene o, en su caso, desde la recepción de la orden de compra. Dicha vigencia rige hasta que el funcionario competente dé la conformidad de la recepción de la prestación a cargo del contratista y se efectúe el pago correspondiente.

3.3 REQUISITOS DE LAS GARANTÍAS

Las garantías que debe presentar el contratista deberán ser incondicionales, solidarias, irrevocables y de realización automática al solo requerimiento de la Entidad, emitida por una empresa autorizada y sujeta al ámbito de supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones o que estén consideradas en la lista actualizada de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

3.4 DE LAS GARANTÍAS

3.4.1 GARANTÍA DE SERIEDAD DE OFERTA

Los postores deberán presentar la garantía de seriedad de oferta a efectos de garantizar la vigencia de su oferta, según el monto establecido en las presentes Bases.

El postor que resulte ganador de la Buena Pro y el que ocupó el segundo lugar están obligados a mantener su vigencia hasta la suscripción del contrato.

Luego de consentida la Buena Pro, la Entidad devolverá las garantías presentadas por los postores que no resultaron ganadores de la Buena Pro, con excepción del que ocupó el segundo lugar y de aquellos que decidan mantenerlas vigentes hasta la suscripción del contrato.

El plazo de vigencia de la garantía de seriedad de oferta no podrá ser menor a dos (2) meses computados a partir del día siguiente de la presentación de las propuestas. Esta garantía puede ser renovada.

3.4.2 GARANTÍA DE FIEL CUMPLIMIENTO

El postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del contrato. Esta deberá ser emitida por una suma equivalente al diez por ciento (10%) del monto del contrato original y tener vigencia hasta la conformidad de la recepción de la prestación a cargo del contratista.

De manera excepcional, respecto de aquellos contratos que tengan una vigencia superior a un (1) año, previamente a la suscripción del contrato, las Entidades podrán aceptar que el ganador de la Buena Pro presente la garantía de fiel cumplimiento y de ser el caso, la garantía por el monto diferencial de la propuesta, con una vigencia de un (1) año, con el compromiso de renovar su vigencia hasta la conformidad de la recepción de la prestación.

3.4.3 GARANTÍA POR EL MONTO DIFERENCIAL DE PROPUESTA

Cuando la propuesta económica fuese inferior al valor referencial en más del veinte por ciento (20%) de aquel, para la suscripción del contrato, el postor ganador deberá presentar una garantía adicional por un monto equivalente al veinticinco por ciento (25%) de la diferencia entre el valor referencial y la propuesta económica. Dicha garantía deberá tener vigencia hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.4.4 GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En caso el contrato conlleve a la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorgará una garantía adicional por este concepto, la misma que se renovará periódicamente hasta el cumplimiento total de las obligaciones garantizadas, no pudiendo eximirse su presentación en ningún caso.

3.5 EJECUCIÓN DE GARANTÍAS

Las garantías se harán efectivas conforme a las estipulaciones contempladas en el artículo 164° del Reglamento.

3.6 DE LAS PENALIDADES E INCUMPLIMIENTO DEL CONTRATO

La aplicación de penalidades por retraso injustificado en la atención del bien requerido y las causales para la resolución del contrato, serán aplicadas de conformidad con los Artículos 165° y 168° del Reglamento.

De acuerdo con los artículos 48º de la Ley y 166º del Reglamento, en las Bases o el contrato podrán establecerse penalidades distintas a la mencionada en el artículo 165º del Reglamento, siempre y cuando sean objetivas, razonables y congruentes con el objeto de la convocatoria, hasta por un monto máximo equivalente al 10% del monto del contrato vigente o, de ser el caso, del ítem que debió ejecutarse. Estas penalidades se calcularán de forma independiente a la penalidad por mora.

3.8 PAGOS

La Entidad deberá realizar todos los pagos a favor del contratista por concepto de los bienes objeto del contrato. Dichos pagos se efectuarán después de ejecutada la respectiva prestación; salvo que, por razones de mercado, el pago del precio sea condición para la entrega de los bienes.

La Entidad podrá realizar pagos periódicos al contratista por el valor de los bienes contratados en cumplimiento del objeto del contrato, siempre que estén fijados en las Bases y que el contratista los solicite presentando la documentación que justifique el pago y acredite la existencia de los bienes. Las Bases podrán especificar otras formas de acreditación de la obligación. Los montos entregados tendrán el carácter de pagos a cuenta.

En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

Plazos para los pagos

La Entidad deberá pagar las contraprestaciones pactadas a favor del contratista en la oportunidad establecida en las Bases o en el contrato. Para tal efecto, el responsable de dar la conformidad de la recepción de los bienes, deberá hacerlo en un plazo que no excederá de los diez (10) días calendario de ser éstos recibidos.

En caso de retraso en el pago, el contratista tendrá derecho al pago de intereses conforme a lo establecido en el artículo 48° de la Ley, contado desde la oportunidad en que el pago debió efectuarse.

3.9 DISPOSICIONES FINALES

Todos los demás aspectos del presente proceso no contemplados en las Bases se regirán supletoriamente por la Ley de Contrataciones del Estado y su Reglamento, así como por las disposiciones legales vigentes.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCESO DE SELECCIÓN

(En esta sección la Entidad deberá completar la información exigida de acuerdo a las instrucciones indicadas)

CAPÍTULO I

GENERALIDADES

1.1 ENTIDAD CONVOCANTE

Entidad : **MINISTERIO DE EDUCACIÓN**
Unidad Ejecutora : 024 – Sede Central
Número de RUC : 20131370998
Central Telefónica : 615-5800 - Anexos: 22062 ó 21055

1.2 DOMICILIO LEGAL

Avenida De La Poesía 155. Altura de la cdra. 19 Av. Javier Prado Este. - San Borja - Lima.

1.3 OBJETO DE LA CONVOCATORIA

El presente proceso tiene por objeto la adquisición de antivirus, filtrado de contenidos y antispam para la Sede Central y Sedes descentralizadas del Ministerio de Educación.

1.4 VALOR REFERENCIAL

El valor referencial asciende a **S/. 504,520.80 (Quinientos Cuatro Mil Quinientos Veinte con 80/100 Nuevos Soles),** incluido los impuestos de Ley y cualquier otro concepto que incida en el costo total del bien. El valor referencial ha sido calculado al mes de marzo de 2011.

El valor referencial señalado en el párrafo anterior está desagregado de la siguiente manera:

ITEM	CONCEPTO	UNIDAD	VALOR TOTAL
1	**ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACIÓN**		
1.1	SOFTWARE DE PROTECCION ANTIVIRUS, FILTRADO DE CONTENIDO Y ANTISPAM	1	S/.457,556.80
1.2	SERVIDORES	2	S/.46,964.00
TOTAL			**S/.504,520.80**

1.5 EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución de Secretaría General Nº 0496-2011-ED de fecha 18 de mayo de 2011.

1.6 FUENTE DE FINANCIAMIENTO[6]

Recursos Ordinarios.

1.7 SISTEMA DE CONTRATACIÓN

El presente proceso se rige por el Sistema de Suma Alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.8 ALCANCES DEL REQUERIMIENTO

El requerimiento está definido en el Capítulo III de la presente Sección.

[6] La fuente de financiamiento debe corresponder a aquellas previstas en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el proceso de selección.

1.9 PLAZO DE ENTREGA

El plazo de entrega de los bienes, incluyendo su instalación, configuración y puesta en operación del producto 01 (antivirus) y 03 (filtrado de contenido y antispam) en un plazo no mayor a **sesenta (60) días calendario,** contados **a partir del día siguiente de suscrito el contrato.**

Los bienes serán entregados en los almacenes del Ministerio de Educación en horarios de lunes a viernes de 8:30 a 18:00 horas, en el Almacén Venezuela-MED, situado en la Av. Venezuela Nº 1891 Cercado de Lima, Lima 01 y/o en otro Almacén que la Entidad señale, mismo que estará ubicada en el departamento deLima.

1.10 BASE LEGAL

- Ley N°28411 - Ley General del Sistema Nacional de l Presupuesto.
- Decreto Legislativo N° 1017 – Aprueba la Ley de Co ntrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 184-2008-EF – Aprueba el Reglam ento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo N° 021-2009-EF – Modificación del Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo N° 140-2009-EF – Modificación del Reglamento de la Ley de Contrataciones del Estado.
- Directivas de OSCE
- Ley N°27444 – Ley del Procedimiento Administrativ o General.
- Código Civil.
- Ley 27806 – Ley de Transparencia y de Acceso a la Información Pública
- Decreto Supremo Nº 007-2008-TR, Texto Único Ordenado de la Ley de Promoción de la Competitividad, Formalización y Desarrollo de la Micro y Pequeña y del acceso al empleo decente, Ley MYPE.
- Decreto Supremo Nº 008-2008-TR, Reglamento de la Ley MYPE.

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

Para la aplicación del derecho deberá considerarse la especialidad de las normas previstas en las presentes Bases.

CAPÍTULO II

DEL PROCESO DE SELECCIÓN

2.1 CRONOGRAMA DEL PROCESO DE SELECCIÓN[7]

Convocatoria en el SEACE	El 08/06/2011
Registro de Participantes	Del 09/06/2011 al 12/07/2011
Formulación de Consultas	Del 09/06/2011 al 15/06/2011
Absolución de Consultas	El 21/06/2011
Formulación de Observaciones	Del 22/06/2011 al 28/06/2011
Absolución de Observaciones	El 05/07/2011
Integración de Bases	El 11/07/2011
Presentación de propuestas	18/07/2011 a las **11:00 horas** en la Unidad de Abastecimiento del Ministerio de Educación.
Evaluación de propuestas	Del 19/07/2011 al 20/07/2011
Otorgamiento de la Buena Pro	21/07/2011 a las **16:00 horas** en la Unidad de Abastecimiento del Ministerio de Educación.

2.2 REGISTRO DE PARTICIPANTES Y ENTREGA DE BASES

El registro de los participantes se realizará en la Sede Central del Ministerio de Educación, sito en la Av. De la Poesía 155 San Borja, en las fechas señaladas en el cronograma, en el horario y en las fechas señalado en el cronograma, en el horario de 8:30 horas a 17:00 horas, previo pago de la suma **S/.5.00 (Cinco con 00/100 Nuevos Soles**) por derecho de participación.

En el momento de la entrega de las Bases al participante, se emitirá la constancia o cargo correspondiente en la que constará: el número y objeto del proceso, el nombre y firma de la persona que recibe las Bases así como el día y hora de dicha recepción.

2.3 FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

Las consultas y observaciones se presentarán por escrito, debidamente fundamentadas, ante la ventanilla de Mesa de Partes de la Entidad, sito en *la Av. De la Poesía 155 San Borja*, en las fechas señaladas en el cronograma, en el horario de *8:30 horas a 17:00 horas*[8], debiendo estar dirigidos al Presidente del Comité Especial de la **LICITACIÓN PÚBLICA N°006-2011-ED/UE 024,** pudiendo acompañar **opcionalmente** un cd conteniendo las consultas y/u observaciones.

MUY IMPORTANTE, no se absolverán consultas a las Bases que se presenten extemporáneamente, que sean formuladas por quienes no se han registrado como participantes o que hayan sido ingresadas en una Mesa de Partes distinta a la de la Sede Central del Ministerio de Educación.

---

[7] La información del cronograma indicado en las Bases no debe diferir de la información consignada en el cronograma de la ficha del proceso en el SEACE. No obstante, de existir contradicción en esta información, primará el cronograma indicado en la ficha del proceso en el SEACE.

[8] Las Entidades de preferencia, deberán establecer que en el horario de atención al público se presentarán las consultas y observaciones, de lo contrario, deberán contemplar un horario razonable para la formulación de éstas, de modo que se fomente la mayor participación de postores, en concordancia con el Principio de Libre Concurrencia y Competencia.

2.4 ACTO PÚBLICO DE PRESENTACIÓN DE PROPUESTAS

Las propuestas se presentarán en **Acto Público** a realizarse en la Unidad de Abastecimiento del Ministerio de Educación, sito, **Avenida De La Poesía Nº 155, distrito de San Borja, provincia y departamento de Lima (altura de la Cuadra 19 de la Av. Javier Prado Este)**, en la fecha y hora señalada en el cronograma. El acto público se realizará con la participación de Notario.

Se podrá contar con la presencia de un representante del Sistema Nacional de Control, quien participará como veedor y deberá suscribir el acta correspondiente. La no asistencia del mismo no vicia el proceso.

Las propuestas se presentarán en dos (2) sobres cerrados y estarán dirigidas al Comité Especial del **LICITACIÓN PÚBLICA N° 006-2011-ED/UE 024,** conforme al siguiente detalle:

SOBRE N°1: Propuesta Técnica. El sobre será rotulado:

Señores
NOMBRE DE LA ENTIDAD
DIRECCIÓN
Att.: Comité Especial
LICITACIÓN PÚBLICA N°006-2011-ED/UE 024
Objeto del proceso: Adquisición de antivirus, filtrado de contenidos y antispam para la Sede Central y Sedes descentralizadas del Ministerio de Educación.

SOBRE N°1: PROPUESTA TÉCNICA
NOMBRE / RAZON SOCIAL DEL POSTOR

SOBRE Nº 2: Propuesta Económica. El sobre será rotulado:

Señores
NOMBRE DE LA ENTIDAD
DIRECCIÓN
Att.: Comité Especial
LICITACIÓN PÚBLICA N°006-2011-ED/UE 024
Objeto del proceso: Adquisición de antivirus, filtrado de contenidos y antispam para la Sede Central y Sedes descentralizadas del Ministerio de Educación.

SOBRE N°02: PROPUESTA ECONÓMICA
NOMBRE / RAZON SOCIAL DEL POSTOR

2.5 CONTENIDO DE LAS PROPUESTAS

SOBRE Nº 1 - PROPUESTA TÉCNICA:

Se presentará en un (1) original y dos copias[9]

El Sobre N° 1 contendrá, además de un índice de documentos[10], la siguiente documentación:

[9] De acuerdo con el artículo 63º del Reglamento, la propuesta técnica se presentará en original y en el número de copias requerido en las Bases, el que no podrá exceder de la cantidad de miembros que conforman el Comité Especial.

[10] La omisión del índice no descalifica la propuesta, ya que su presentación no tiene incidencia en el objeto de la convocatoria.

Documentación de presentación obligatoria:

a. Copia simple del Certificado de inscripción vigente en el Registro Nacional de Proveedores: Capítulo de Bienes. Cuando se trate de Consorcio, el certificado será presentado por cada uno de los miembros que conforman el consorcio.

b. Declaración Jurada de datos del postor.
Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados - **Anexo Nº 01.**

c. Declaración jurada de cumplimiento de los Requerimientos Técnicos Mínimos contenidos en el Capítulo III de la presente sección[11], **en la que se señale la marca y modelo de los servidores incluidos en la presente adquisición, Anexo Nº 02.** Cuando se trate de Consorcio, ésta declaración jurada será presentada por cada una de las empresas que conforman el consorcio.

Además deberá presentar:

1. Características de los servidores incluidos en la presente adquisición.
Todos los documentos que contengan información esencial de las propuestas se presentarán en idioma castellano o, en su defecto, acompañados de traducción efectuada por traductor público juramentado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que se encuentren contenidas en idioma distinto al castellano, deberá ser presentada en el idioma original y podrá contar con traducción no oficial. El postor será responsable de la exactitud y veracidad de dichos documentos. La omisión de la presentación del documento o su traducción no es subsanable.

2. Documentación expedida por el fabricante, que acredite que el proveedor y nuestra entidad contarán con el respaldo total del mismo para el soporte directo, en caso de incidencias de malware y filtrado de contenido.

3. Personal certificado en la solución que oferta, éstos certificados deberán ser expedidos por el fabricante de antivirus y el fabricante de filtrado de contenidos, para efectos de despliegue, soporte y mantenimiento de la solución.

4. Certificados y/o constancias que acredite que cuentan con una persona con conocimientos en proyecto.

5. Currículo Vitae documentado (copia simple) del personal que implementará la solución.

d. Declaración jurada simple de acuerdo al Artículo 42º del Reglamento de la Ley de Contrataciones del Estado[12] - **Anexo Nº 03**. Cuando se trate de Consorcio, ésta declaración jurada será presentado por cada una de las empresas que conforman el consorcio.

---

[11] La Entidad deberá precisar si solo bastará la presentación de una declaración jurada para acreditar el cumplimiento de los requerimientos técnicos mínimos o, si será necesario que lo declarado se encuentre respaldado con la presentación de algún otro documento, en cuyo caso, deberá precisarse dicha información en este literal.

En este último caso, debe tenerse en cuenta que podrá solicitarse documentos tales como formatos, certificados, constancias o cualquier otro que sea necesario para acreditar los requerimientos técnicos mínimos, siempre en concordancia con el expediente de contratación y en observancia de los Principios de Economía, de Libre Concurrencia y Competencia y de Trato Justo e Igualitario establecidos en el artículo 4º de la Ley de Contrataciones del Estado.

[12] En este documento se encuentra incluida la declaración jurada sobre el compromiso de mantener vigente la oferta del postor hasta la suscripción del contrato, conforme a lo requerido por el artículo 157º del Reglamento.

e. Promesa de consorcio, de ser el caso, consignando los integrantes, el representante común, el domicilio común y el porcentaje de participación. **Anexo Nº 04**

La promesa formal de consorcio deberá ser suscrita por cada uno de sus integrantes. En caso de no establecerse en la promesa formal de consorcio las obligaciones, se presumirá que los integrantes del consorcio ejecutarán conjuntamente el objeto de convocatoria, por lo cual cada uno de sus integrantes deberá cumplir con los requisitos exigidos en las Bases del proceso.

f. Se presume que el representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al proceso de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.

Muy importante:

La omisión de alguno de los documentos enunciados acarreará la descalificación de la propuesta.

Documentación de presentación facultativa:

a) Copias de comprobantes de pago, contratos u ordenes de compra que acrediten experiencia del postor conforme a las condiciones precisadas en el factor de evaluación "Experiencia del Postor" del capitulo V de las Bases.
b) Declaración Jurada de Experiencia del postor, según **Anexo Nº 06.**
c) Declaración Jurada de mejoras, según el **Anexo Nº 07**.

SOBRE N°2 - PROPUESTA ECONÓMICA

El Sobre N°2 deberá contener la siguiente informac ión obligatoria:

a) Oferta económica y el detalle de precios de la prestación principal (Equipos Informáticos) como de las prestaciones accesorias (mantenimiento preventivo), señalando además el monto total. (Anexo **Nº 06**)

La propuesta económica debe ser expresada por un monto fijo integral.

El monto total de la propuesta económica y los subtotales que lo componen deberán ser expresados con dos decimales. Los precios unitarios podrán ser expresados con más de dos decimales.

b) Garantía de seriedad de oferta por un monto equivalente al uno por ciento (1%) del valor referencial, materializada en la presentación de una Carta fianza de acuerdo al siguiente detalle:

Carta fianza por la suma de S/. 5,045.21 (Cinco Mil Cuarenta y Cinco con 21/100 Nuevos Soles, como garantía de seriedad de oferta equivalente al uno por ciento (1%) del valor referencial.

Nota:
Las Cartas Fianza deben señalar expresamente que corresponden a una Garantía de Seriedad de la oferta, denominación y número del proceso de selección.

El plazo de vigencia de la garantía de seriedad de oferta **no podrá ser menos de dos (2) meses**, computados a partir del día siguiente a la presentación de propuestas. Estas garantías pueden ser renovadas. La falta de renovación genera la descalificación de la oferta económica o, en su caso, que se deje sin efecto la Buena Pro otorgada.

Una vez suscrito el contrato el monto de la garantía será devuelto al postor, sin dar lugar al pago de intereses. En caso de la no suscripción del contrato por causas imputables al adjudicatario de la Buena Pro, se ejecutará la garantía en su totalidad, una vez que quede consentida la decisión de dejar sin efecto la Buena Pro.

2.6 Determinación del Puntaje Total

Una vez evaluadas las propuestas técnica y económica se procederá a determinar el puntaje total de las mismas.

El puntaje total de las propuestas será el promedio ponderado de ambas evaluaciones, obtenido de la siguiente fórmula:

$$PTPi = c1\ PTi + c2\ PEi$$

Donde:
PTPi = Puntaje total del postor i
PTi = Puntaje por evaluación técnica del postor i
PEi = Puntaje por evaluación económica del postor i
c1 = Coeficiente de ponderación para la evaluación técnica = ***0.70***
c2 = Coeficiente de ponderación para la evaluación económica = ***0.30***

2.7 REQUISITOS PARA LA SUSCRIPCIÓN DEL CONTRATO

Adicionalmente, conforme al artículo 141º del Reglamento y en concordancia con el objeto de la convocatoria, podrá requerirse, entre otros, los siguientes documentos[13]:

a) Copia de DNI del Representante Legal;
b) Copia de la vigencia del poder del representante legal de la empresa;
c) Copia de la constitución de la empresa y sus modificatorias debidamente actualizado;
d) Copia del RUC de la empresa;
e) Código de Cuenta Interbancario (CCI), de corresponder

Asimismo, el postor ganador de la buena pro deberá presentar una carta fianza[14] para efectos de garantizar lo siguiente[15]:

- El fiel cumplimiento del contrato
- El monto diferencial de la propuesta (de ser el caso).
- Por prestaciones accesorias (de ser el caso).

2.8 PLAZO PARA LA SUSCRIPCIÓN DEL CONTRATO

El postor ganador de la buena pro deberá presentar toda la documentación requerida para la suscripción del contrato en el **plazo de cinco (05) días hábiles**. La citada documentación deberá ser presentada en Mesa de Partes del Ministerio de Educación. Sito en Av. De la Poesía 155 Distrito de San Borja.

2.10 PLAZO PARA EL PAGO

La Entidad se compromete a efectuar el pago al contratista en un plazo máximo de diez (10) días calendario siguientes de otorgada la conformidad de recepción de la prestación.

---

[13] Cada Entidad deberá definir si solo requerirá de la presentación de estos documentos o adicionar algún otro.

[14] De acuerdo con el artículo 155º del Reglamento, modificado por Decreto Supremo Nº 021-2009-EF, la Entidad debe señalar expresamente el tipo de garantía que debe otorgar el contratista para la suscripción del contrato.

[15] En cada caso, la Entidad deberá describir las clases y tipos de garantías que deben ser presentadas por el ganador de la Buena Pro para la suscripción del contrato.

2.11 FORMA DE PAGO

"LA ENTIDAD" se obliga a pagar la contraprestación a **"EL CONTRATISTA"** en una sola armada (En Nuevos Soles).

Para el pago, **"EL CONTRATISTA"** deberá presentar ante el Área de Adquisiciones de **"LA ENTIDAD"** la siguiente documentación:

1. Factura por el monto total del contrato.
2. Copia de la Orden de Compra.
3. Conformidad técnica emitida por la Oficina de Informática del MED, señalando el cumplimiento de la prestación, de acuerdo a las especificaciones técnicas de las Bases.
4. Conformidad suscrita por el Jefe del Almacén del Ministerio de Educación.

CAPÍTULO III

MINISTERIO DE EDUCACIÓN
REPÚBLICA DEL PERÚ

Secretaria de Planificación Estratégica
Oficina de Informática.

Términos de Referencia

Adquisición de Anti virus para la Sede Central y sedes descentralizadas del Ministerio de Educación.

Febrero – 2011.

INDICE

1. JUSTIFICACIÓN 26

2. FINALIDAD PÚBLICA: 26

3. OBJETIVO GENERAL 26

3.1. OBJETIVO ESPECIFICO 26

4. AMBITO 26

5. PLAZO DE ENTREGA 27

6. SOBRE EL PROVEEDOR. 27

7. VIGENCIA DE LOS COMPONENTES. 28

8. IDIOMA FINAL HACER IMPLEMENTADO. 28

9. LICENCIAMIENTO. 28

10. CAPACITACIÓN. 28

11. DOCUMENTACIÓN. 29

12. SOPORTE. 29

14. NIVELES DE SERVICIO 30

14.1. Antivirus, filtrado de contenido y antispam 30
14.2. Hardware 30

15. SERVICIO DE MANTENIMIENTO Y SOPORTE DE HARDWARE Y SOFTWARE 31

15.1. Mantenimiento Preventivo. 32
15.2. Mantenimiento Correctivo. 32

16. FORMA DE PAGO 32

17. ESPECIFICACIONES TECNICAS: 33

17.1. PRODUCTO 01 – SOFTWARE ANTIVIRUS 33
17.1.1. Eficacia. 33
17.1.2. Actualización de Firmas. 33
17.1.3. Dispositivos Instalados. 33
17.1.4. Sistemas Operativos Soportados. 33
17.1.5. Control de acceso a dispositivos internos de las estaciones de trabajo Host. 34
17.1.6. Certificaciones del Producto. 34
17.1.7. El antivirus para los equipos de computo deberá contar como mínimo las siguientes características: 34
17.1.8. Consola de administración central 37
17.1.8.1. Instalación del Producto en las Estaciones de Trabajo. 38

17.1.8.2. Políticas 38
17.1.8.3. Alertas y Reportes. 39
17.1.8.4. Adicionalmente. 39
17.1.9. Control de Acceso a la Red (Network Access Control). 39
17.1.10. Despliegue. 40
17.1.11. Equipo y Software. 40
17.1.12. Idiomas Admitidos. 40

17.2. PRODUCTO 02 – FILTRADO DE CONTENIDOS Y ANTISPAM 41
17.2.1. Funcionamiento. 41
17.2.2. Licencias 41
17.2.3. Forma de integración 41
17.2.4. Trazas de filtrado 42
17.2.5. Actualización de trazas 42
17.2.6. Especialización 42
17.2.7. Actualización del software 42
17.2.8. Tipos de filtrado 42
17.2.9. Filtrado 42
17.2.10. Concurrencia de usuarios 43
17.2.11. Manejo de listas 43
17.2.12. Contención de abusos 43
17.2.13. Sistemas operativos 43
17.2.14. Categorización 43
17.2.15. Certificaciones del Producto. 43
17.2.16. Actualizaciones URL y Software. 43
17.2.17. Personalización 43
17.2.18. Políticas. 43
17.2.19. Manuales de ayuda del producto 44
17.2.20. Excepciones 44
17.2.21. Administración 44
17.2.22. Idioma (interfase) 44
17.2.23. Idioma (filtrado) 44
17.2.24. Localización 44
17.2.25. Alertas 44
17.2.26. Reportes 45
17.2.27. Protección de correo electrónico (Antispam). 45
17.3. Instalación y operación 49
17.4. Plataforma 49

TERMINOS DE REFERENCIA PARA LA ADQUISICION DE LA SOLUCION DE ANTI VIRUS PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACION

1. JUSTIFICACIÓN

Ante el incremento significativo de ataques informáticos a través de códigos maliciosos que pueden poner en riesgo la información mantenida en los equipos informáticos del Ministerio de Educación la cual tiene un valor incalculable, se requiere de una solución de seguridad informática que prevenga las filtraciones de códigos no deseados a las redes de datos, servidores y estaciones de trabajo, para mantener la disponibilidad, integridad y confidencialidad de la información.

Por consiguiente, se requiere de una solución de defensa que incorpore un sistema de protección contra los códigos no deseado, que asimismo permita disminuir el riesgo de incidentes de seguridad en sus entornos informáticos, mitigando pérdidas de horas de trabajo, como resultado de la interrupción de las operaciones del Ministerio de Educación.

2. FINALIDAD PÚBLICA:

Brindar un servicio integro, disponible y confidencial de la información a los usuarios a quienes se les brinda el servicio de informática, tanto a las áreas administrativas y pedagógicas, así como a los docentes y alumnos, obteniendo su confianza a través de una solución contra ataques maliciosos, logrando prevenir y corregir, mitigando los riesgos de pérdida, modificación, sustracción de la información y filtración de páginas web no permitidas, que se encuentran en las estaciones de trabajo, servidores y en la red de datos; LAN, WAN e Internet del Ministerio de Educación.

3. OBJETIVO GENERAL

Mejorar el nivel de seguridad contra ataques maliciosos, distribuyendo soluciones de anti malware en las diferentes capas, con estrategias diferente según el avance de la penetración del ataque.

3.1. OBJETIVO ESPECIFICO

Adquirir una solución que brinde las herramientas para la protección y corrección de ataques que puedan dañar la información que es mantenida en la estaciones de trabajo y servidores.

4. AMBITO

El ámbito a que se circunscribe la presente convocatoria son las siguientes locaciones entre otras no menos importantes:

Nº	Sede	Dirección
1	Central – Local ex Centromín	AV. DE LA POESÍA Nº 155, SAN
2	Museo de la Nación	AV. JAVIER PRADO ESTE Nº 2465, SAN BORJA
3	local Ex-Concytec.	CALLE DEL COMERCIO Nº 197, SAN BORJA
4	Pronafcap	AV. SAN LUIS Nº 2276, SAN BORJA
5	Promolibro	CALLE MORELLI Nº 438, SAN BORJA
6	Procuraduría	JR. SÁNCHEZ CERRO N°2150, JESÚS MAR ÍA
7	OBEC	CALLE TIZIANO N°387, SAN BORJA
8	Carabaya	JR. CARABAYA Nº 650, LIMA CERCADO
9	Biblioteca Nacional	AV. DE LA POESÍA Nº 160, SAN BORJA

10	Coneau	San Isidro - Lima
11	Coneaces	San Borja - Lima
12	IPEBA	San Isidro - Lima
13	AREA DE IMPRENTA	AV. LA MOLINA CDRA. 4 S/N
14	Casa de la Literatura	Jr. Ancash 207 – Lima
15	Pronama	San Borja – Lima
16	FONDED	San Borja – Lima
17	Concejo Nacional de Educación	Jesus María - Lima
17	UGEL 02	Lima – Perú
18	UGEL 03	Lince – Lima
19	UGEL 04	Comas – Lima
20	UGEL 05	San Juan de Lurigancho – Lima
21	UGEL 06	Vitarte - Lima

Cuadro Nº 01

Para las demás Sedes, el proveedor prepara los manuales para su instalación, configuración y uso del antivirus:

Información adicional: El Ministerio de Educación cuenta con un servicio de internet de 80 Mbps y 30 Mbps en la red WAN, en algunos casos el MED aumenta el ancho de banda (160 Mbps – Internet y 80 Mbps – WAN),

5. PLAZO DE ENTREGA.

- El proveedor deberá instalar, configurar y dejar puesto en operación el producto 01 (antivirus) y 02 (filtrado de contenido y antispam) en un plazo no mayor de 60 días calendarios contados a partir del día siguiente de la firma de contrato.

6. SOBRE EL PROVEEDOR.

- El proveedor debe contar con el respaldo total del fabricante, para el soporte directo al proveedor, asimismo para la institución contratante, en caso de incidencias de malware y filtrado de contenido, para ello deberá presentar algún documento que acredite el respaldo del fabricante.
- Para efectos del despliegue, soporte y mantenimiento de la solución a ofertar, el proveedor deberá contar con personal certificado por el fabricante de la solución a ofertar, para esto se deberá presentar:
  - Un certificado por el fabricante de antivirus
  - Un certificado por el fabricante de filtrado de contenidos
- El postor deberá contar con una persona que tenga conocimiento en proyectos, para el inicio de la implementación (actividades, cronograma, supervisión e informe final)
- El Postor deberá indicar el staff de personas que trabajaran para esta solución.
- El Ministerio de Educación se reserva el derecho de comprobar la veracidad de esta información.

7. VIGENCIA DE LOS COMPONENTES.

La vigencia del contrato de los productos será por dos años calendarios (2x365 días) como mínimo, el inicio de la vigencia se contará a partir de la fecha del acta de conformidad final y aprobación de la implementación completa por parte de la Oficina de Informática.

8. IDIOMA FINAL HACER IMPLEMENTADO.

La solución deberá de estar configurada e instalada en el idioma Español, dado que este es un producto de usuario final, no se aceptará en ningún otro idioma, sin embargo puede contener aparte del español otros idiomas.

9. LICENCIAMIENTO.

El Ministerio de Educación es respetuoso de la propiedad intelectual, en tal sentido, el proveedor brindará y pondrá a disposición del Ministerio de Educación siempre la última versión o release del producto ofertado disponible en el mercado hasta el tiempo que dure el contrato, la misma que tendrá que ser instalada o actualizada donde se requiera (estaciones de trabajo y servidores), la que tendrá las mismas condiciones del producto ofertado, estas licencias podrían ser para gobierno, corporativas o para educación, el software deberá ser privativo o comerciales.

10. CAPACITACIÓN.

- El postor deberá capacitar el personal del Ministerio de Educación en dos grupos, el primer grupo estará conformado por los técnicos de soporte a usuarios y el segundo grupo por los especialistas del Centro de Datos.
- El grupo de técnicos de soporte estará conformados por un mínimo de 18 personas, a los cuales se les dará capacitación en dos sub-grupos de 9 personas de forma que no afecten las labores del Ministerio de Educación.
- El grupo de especialistas estará conformado por 15 personas a las cuales se les dará capacitación en 02 sub-grupos de forma que no afecten las labores del Ministerio de Educación.
- La capacitación de los técnicos de soporte será dictada fuera de horario de labores, por un periodo de **8 horas** lectivas y en los ambientes de la sala de capacitación del Ministerio de Educación, en esta capacitación se incidirá con mayor énfasis a los temas de las pruebas de despliegue, configuración y resolución de incidentes de la solución.
- La capacitación de los especialistas del centro de Datos será dictada fuera de horario de labores, por un periodo de **8 horas** lectivas y en los ambientes proporcionados por el postor en el cual deberá de ofrecer los equipos necesarios para efectuar dentro de la capacitación sobre la instalación, y manejo de la solución; las pruebas de configuración y resolución de incidentes de la solución.
- El instructor o los instructores designados por el postor deberán estar certificados por el producto que presente, debiendo presentar entre los dos instructores los certificados tanto de antivirus y filtrado de contenido.
- El proveedor una vez realizado la capacitación deberá tomar un examen de evaluación al personal que ha recibido el curso.
- Al finalizar los periodos de entrenamiento, el postor deberá otorgar un certificado de capacitación por cada producto ofertada tanto en administración del sistema y otro de soporte técnico (en antivirus y filtrado de contenido), se deja constancia que la capacitación debe dejar al personal entrenado apto para optar por el examen de certificación de la marca.

11. DOCUMENTACIÓN.

Al final del procedimiento de Instalación en los equipos y estaciones de trabajo, el postor deberá entregar un manual detallado paso a paso de la solución Implementada en el Ministerio de Educación, elaborando un Informe Final de la Implementación de la solución y de las condiciones en que las deja operando, lo cual servirá para su conformidad de servicio realizado.

La siguiente información deberá ser presentada dentro del plazo de entrega de los bienes e implementación de los servicios:

- Documentación propia de los equipos y del software propuesto.
- Descripción técnica general de los equipos y software, especificando su arquitectura.
- Manuales de Instalación (software).
- Manuales de configuración y operación, (software).
- Una vez terminada la instalación de toda la solución, el proveedor deberá entregar un informe final de la instalación del hardware, software e implementación del diseño, indicando como mínimo:
- Un mapeo de la configuración de los esquemas de cada componente de la solución, adjuntando documentación relevante y las pruebas realizadas.
- El informe final deberá contener los procedimientos que garanticen la disponibilidad y continuidad de la solución.
- Toda la documentación proporcionada por el postor deberá suministrarse en forma impresa y digital (01 CD/DVD).

12. SOPORTE.

- El postor deberá contar con tres (03) personas de soporte técnico certificado por el fabricante, los mismos que deberán presentar un certificado de cada solución, por ejemplo (un certificado de antivirus y dos de filtrado de contenido) o (un certificado de filtrado de contenido y dos de antivirus), adicionalmente habrá un encargado o responsable de filtrado de contenido y antivirus, quien será el nexo con el MED.
- El postor deberá contar con soporte local y del fabricante.
- El personal técnico propuesto por el postor, es quien dará el soporte técnico al Ministerio de Educación, si el proveedor cambiara uno de los técnicos tendrá que demostrar que cumple con los términos de referencia ofertada.
- El postor asignara a un especialista para las coordinaciones de los proyectos a realizarse referente al antivirus y filtrado de contenido.
- Deberá Incluir el servicio de despliegue llave en mano (sede-del-MED), según diagrama de Red del MED con su personal.
- El postor para una mejor comunicación con el encargado de la consola de atención deberá proporcionar un equipo del tipo Smartphone de última generación que permita la comunicación ilimitada con el proveedor, envío de mensajes de texto y/o correo electrónico, con la finalidad de reportar todas las incidencias.
- Una vez finalizado el tiempo del contrato, el equipo referido en el párrafo precedente será devuelto al postor.
- En caso de pérdida del equipo por parte del operador de la consola, este deberá reponer el equipo y sufragar todos los gastos ocasionados.
- El postor deberá considerar un seguro para el equipo que considere su reposición en caso de pérdida, considerando un esquema de valorización descendente según sea el plazo a contratar.
- Proporcionará soporte telefónico y por Web ilimitado para los productos incluidos en la propuesta durante el periodo de garantía.
- El proveedor proporcionará asistencia de soporte del fabricante a través de la página Web del mismo.
- Con el servicio de soporte el proveedor deberá asegurarse que los equipos queden

plenamente operativos, con las óptimas medidas de seguridad y performance en la Red.
- El proveedor no podrá poner límite a la cantidad de consultas o solicitudes efectuadas por el personal del Ministerio de Educación.
- El postor debe contar una línea directa para realizar las llamadas de atención.
- El postor deberá efectuar una revisión mensual de la solución Instalada, elaborando informe de la situación encontrada e incidentes de seguridad reportadas y atendidas o en proceso.
- Deberá proveerse un número telefónico de contacto (call center), que opere en un esquema 12 x 5 (doce horas, de 8 am a 8 pm, de lunes a viernes).
- El proveedor en caso de ocurrir un problema suscitado por cualquier tipo de vulnerabilidad producido por un virus o malware o del filtrado de contenido, el proveedor asistirá en el soporte las 24 horas x 7 días a la semana hasta que dure el contrato, para esto el proveedor dará un número de celular para este servicio.
- Se debe realizar una vez al año a solicitud de la OFIN de un Mantenimiento Preventivo de la solución integral ofertada, tanto a nivel de Hardware y Software.

14. NIVELES DE SERVICIO

14.1. Antivirus, filtrado de contenido y antispam

- Soporte On-site y On-Line en modo 7 x 24x 365 durante el periodo de vigencia del contrato.
- Si en caso la llamada realizada por el personal de soporte técnico, no tuviera éxito en contactarse, se procederá por un correo electrónico que deberá asignar el proveedor para la atención inmediata, una vez realizo el envió el proveedor tendrá que devolver la llamada en un tiempo máximo de 15 minutos.
- Si la incidencia suscitada producto de un evento pueda solucionarse por vía telefónica u otro medio, el proveedor tendrá un tiempo máximo de 30 minutos. Para dar la solución.
- Si la incidencia escalara a un problema, el proveedor tendrá un tiempo máximo de 04 horas para el diagnóstico.
- Si el problema fuera suscitada por un nuevo virus o alguna vulnerabilidad de la solución de seguridad del contrato, el proveedor tendrá un tiempo de respuesta de 02 horas como máximo, para las actualizaciones correspondientes.
- En caso que la vulnerabilidad encontrada tuviera un impacto negativo, la misma que fueran afectadas las estaciones de trabajo y servidores, el proveedor deberá corregir y actualizar el antivirus así como la solución del filtrado, asimismo realizara el despliegue de todos los recursos necesarios incluyendo al personal para asegurar que el virus no se encuentran en las estaciones de trabajo y continuar con las operaciones del MED, esta es una excepción que tendrá un plazo de 6 horas para culminar.
- La presencia de los especialistas ofertados, se dará cuando el problema lo requiera o a solicitud de la entidad, este se deberá presentar en tiempo máximo de 02 horas, luego de efectuada la llamada o de enviada la solicitud.
- El proveedor deberá clasificar las incidencias que pudieran suscitar de este servicio, en coordinación con el personal técnico de OFIN, en un plazo de 30 días después de la firma de contrato.
- El proveedor deberá dar solución a cualquier evento en menos de 08 Horas, desde cuando ocurrió la llamada.

14.2. Hardware

- **Reemplazo de componentes.-** Si cualquier componente de los bienes adquiridos, que forman parte de la solución ofertada, quedase inoperativo, o mantuviera un funcionamiento defectuoso de hasta en tres (03) ocasiones durante un periodo

de ciento veinte (120) días calendarios; el proveedor deberá reemplazar dicha parte, bien por otro igual o de mejores características, sin costo alguno para el Ministerio de Educación.

- **Tiempo de Respuesta.-** Como tiempo de respuesta se define el período desde que se genera la orden del servicio por parte del Ministerio de Educación, hasta el instante en que el técnico designado por el proveedor tome contacto con los funcionarios encargados de la administración y/u operación de la plataforma que integra la solución, el cual no excederá de 2 horas.

- **Tiempo de Solución.-** Como tiempo de solución, se define el período desde que se genera la orden de servicio por parte del Ministerio de Educación, hasta el instante en que el técnico designado por el proveedor deje en forma operativa y funcionando en forma eficiente, el componente de la solución reportado con falla, Este tiempo no deberá exceder las 06 horas.

- **Cobertura Horaria.-** El horario de atención solicitado será en modalidad de Horario Extendido, es decir con una cobertura de 24 horas del día, los 7 días de la semana, los 365 días del año.

- **Costos incluidos.-** El proveedor deberá considerar en la elaboración de su propuesta, todos los costos del equipamiento, software, servicios de instalación y cumplimiento de la garantía (mantenimiento y soporte) y los costos adicionales, si hubieran (traslados, seguros, insumos, etc.)

- **Traslado.-** En caso de que fuese necesario trasladar o movilizar equipos, módulos, partes y tarjetas objeto del contrato, serán entera responsabilidad de la empresa que brinda el servicio.

15. SERVICIO DE MANTENIMIENTO Y SOPORTE DE HARDWARE Y SOFTWARE

Son las actividades de carácter obligatorio asociadas al mantenimiento preventivo y correctivo de los componentes de hardware y software que conforman la solución durante el período de vigencia de la garantía otorgada por el proveedor.

Estas actividades incluyen, al menos:

- Realizar diagnósticos de hardware y software.
- Instalar service packs, hot fixes, microcódigos, firmware y mantenimiento de las versiones de software base si lo requiere.
- Actualización de la versión de software.
- Reemplazar componentes defectuosos, incluyendo el correspondiente mantenimiento preventivo de acuerdo a lo requerido.
- Reemplazar equipos completos por deficiencias incorregibles en el funcionamiento o inoperatividad definitiva.
- Planificar las interrupciones de los servicios debido al mantenimiento planeado u otras actividades que se han necesarias.
- Informar oportunamente al Ministerio de Educación de las actividades a realizarse con 10 días de anticipación.

Estos servicios de Mantenimiento y Soporte de Hardware y Software, deberán ser efectuados por personal debidamente certificado por el producto, y sin costo adicional para el Ministerio de Educación que el ofertado en su propuesta.

15.1. Mantenimiento Preventivo.

El servicio de Mantenimiento Preventivo se realizará una vez al año durante el periodo de garantía (dos años), sin costo alguno adicional para el Ministerio de Educación que el estipulado en la propuesta del proveedor y comprende las siguientes actividades mínimas básicas:

- Servicio de diagnóstico limpieza interna, externa y reconocimiento del buen funcionamiento (test) de los equipos.
- Pruebas de operación de los servicios que se ejecutan en los equipos involucrados.
- El horario y días para realizar este mantenimiento preventivo, será previa aceptación de la Oficina de Informática del MED.

15.2. Mantenimiento Correctivo.

Se efectuará a demanda, sin costo adicional para el Ministerio de Educación y comprende las siguientes actividades mínimas:

- Atención de requerimientos o incidentes técnicos en el horario señalado (7x24x365).
- Servicio de diagnóstico, test y reparación de los equipos.
- La solución será hasta poner operativo el componente.
- Reemplazar componentes y/o piezas defectuosas.
- Asegurar y proveer los repuestos, equipos, dispositivos, software, componentes y/o piezas necesarios para garantizar un máximo nivel de disponibilidad de los equipos, y restaurar a éstos su funcionamiento óptimo cuando una falla o irregularidad se produzca.
- El reemplazo de equipos, módulos, partes, piezas, tarjetas, cables, etc. será con equipos y partes nuevas: módulos, partes, piezas, tarjetas, cables de iguales o de mejores características tecnológicas.
- Las solicitudes para realizar el mantenimiento correctivo de los equipos, se llevarán a cabo mediante una llamada telefónica o un email al proveedor del servicio, el cual generará un código, que lo identifique y registre el día y la hora. El tiempo de respuesta máximo de atención es de 2 horas.
- Si el equipo, (módulos, partes, piezas, tarjetas, cables, etc) no hubiera sido reparado dentro de las 06 horas hábiles contadas desde la llamada de la Sede Central, el contratista deberá instalar temporalmente en la sede del MED un componente similar, hasta ejecutar la solución definitiva.

16. FORMA DE PAGO

- Los pagos se ejecutara previa presentación del acta de conformidad emitida por la Oficina de Informática.
- El pago será al 100% del monto ofertado, unas vez cumplido la instalación e implementación del filtrado de contenido y antivirus.

17. ESPECIFICACIONES TECNICAS:

17.1. PRODUCTO 01 – SOFTWARE ANTIVIRUS

CANTIDAD A ADQUIRIR: 2,000 Licencia

17.1.1. Eficacia.

La solución debe proveer de un mecanismo de detección proactiva ante amenazas conocidas que detecten virus, adware, malware y spyware "antes de su ejecución".

17.1.2. Actualización de Firmas.

Se denomina actualización de firmas al paquete de programas que actualizan desde Internet el producto instalado en los Servidores y estaciones de trabajo del usuario; en este sentido la actualización constante del producto instalado en los citados equipos, con el nuevo release o última actualización disponible en el mercado, durante el periodo de vigencia del contrato, permitirá una adecuada protección de la Red Informática Interna del Ministerio de Educación y debe tener como mínimo una periodicidad de descarga de cuanto menos cada una hora, esta descarga deberá ser canalizada a través de un equipo servidor de descargas a la cual los equipos servidores y estaciones de trabajo acudirán para su actualización, en las sedes externas. El producto deberá permitir repositorios externos, asimismo deberá permitir también su actualización directa desde internet.

17.1.3. Dispositivos Instalados.

El Ministerio de Educación tiene instalado un equipo Firewall basado en software Squid que hará enlace de la solución ofrecida por el proveedor con el Router de salida a Internet.

17.1.4. Sistemas Operativos Soportados.

Sistemas soportados para las estaciones de trabajo y servidores, este requerimiento es necesario por la variedad de sistemas operativos que mantienen las Direcciones Regionales y Unidades de Gestión Educativas.

- Sistemas operativos Windows para estación de trabajo (**en adelante: Windows**), los cuales comprenden:

  - ✓ Microsoft Windows 7
  - ✓ Microsoft Windows Vista
  - ✓ Microsoft Windows Vista x64
  - ✓ Microsoft Windows 2000 Professional (Service Pack 4 o superior)
  - ✓ Microsoft Windows XP Professional (Service Pack 1 o superior)

- Sistemas operativos para servidor de archivos (en adelante: **Windows Server**), los cuales comprenden:

  - ✓ Microsoft Windows 2000 Professional / Professional SP1 o superior
  - ✓ Microsoft Windows Server 2003
  - ✓ Microsoft Windows Server 2003 x64
  - ✓ Microsoft Windows Server 2008
  - ✓ Microsoft Windows Server 2008 x64

- Sistemas operativos Linux (en adelante: **Linux),** los cuales comprenden:

  - ✓ Fedora 9 (kernel 2.6.25)
  - ✓ SUSE Linux Enterprise Server
  - ✓ Ubuntu 10 Desktop Edition
  - ✓ Red Hat Enterprise Linux 5.2 Server
  - ✓ Centos 5.4 o superior

17.1.5. Control de acceso a dispositivos internos de las estaciones de trabajo Host.

- El producto a adquirir debe permitir al operador responsable de toda la solución (Administrador del Sistema), bloquear u autorizar el manejo de los dispositivos de E/S, tales como Memorias USB, Grabadores de CD/DVD, Disquetera, Discos Duros externos, todas estas actividades deberán realizarse desde una consola de Administración, mediante la aplicación de políticas de bloqueo o desbloqueo.

- Todos los eventos de incidencias de malware el sistema de control de acceso a dispositivos deberá ser reportado a la consola de administración centralizada con la finalidad de permitir la creación de reportes ejecutivos del uso de este tipo de dispositivos en la red del Ministerio de Educación.

17.1.6. Certificaciones del Producto.

El producto a ofertar debe estar incluido en el cuadrante mágico de Gartner de plataformas de protección de punto final, ultima publicación por esta empresa independiente de los últimos dos años, para tal efecto el postor deberá acompañar los gráficos correspondientes, además de la certificación o documento que acredite que se han realizado pruebas sobre el producto como ICSALABS o CASCADIA LABS.

17.1.7. El antivirus para los equipos de computo deberá contar como mínimo las siguientes características:

- Protección contra código malicioso que cubra al menos virus, troyanos, gusanos y programas no deseados.
- Prevención de ataques de hackers mediante la incorporación de un firewall personal de última generación, que incluya un IDS o IPS (sistema de detección o prevención de intrusos).
- Contar con actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando de esta manera que pueda afectar los recursos de ancho de banda de la red.
- Contar con el soporte para IPV6.
- Contar con un disco de rescate.
- Diseñada para funcionar en un ambiente de red, y el mismo fabricante debe proporcionar las herramientas para ser administrada de forma centralizada, tanto para la configuración, como para la instalación y actualizaciones.
- Debe proveer de manejo manual y automático (programado) de la actualización del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo desde Internet, también desde una consola central.
- Debe tener la capacidad de bloquear y autorizar aplicaciones.
- Debe tener la capacidad de poseer un firewall propio.
- Debe permitir la detección sobre todo tipo de archivos incluidos los en formato comprimido.
- Detectar si el antivirus de un equipo está activo y actualizado de modo que en forma automática le permita activarse y actualizarse, si por cualquier razón el sistema antivirus no puede activarse o actualizarse.

- Análisis de Scripts Capacidad para analizar Scripts de JavaScript y VBScript antes de que se ejecuten.
- Debe permitir tener la capacidad para detectar la dirección IP atacante o infectante.
- Deberá escanear y bloquear en tiempo real cualquier acceso e instalación de cualquier spyware, adware, malware, key logger

A. Para Windows estaciones de trabajo o computadora personal el antivirus:

- Debe soportar de manera nativa en los sistemas operativos para estación.
- El antivirus debe ser administrable desde un servidor central.
- Todas las características del antivirus deben poder ser configuradas a través de un servidor central de configuración.
- Debe ser capaz de proporcionar seguridad para sistemas de archivos. Todos los archivos creados, ejecutados o modificados deberán ser escaneados (en busca de contenido malicioso).
- Cualquier archivo individual, directorios y discos (local y red) también deben poder ser escaneados.
- Debe ser capaz de optimizar la demanda de recursos para permitir que el usuario no vea reducida la disponibilidad de recursos del sistema para sus aplicaciones.
- El componente también debe analizar los mensajes entrantes en busca de sitios web fraudulentos (“phishing”).
- Debe contener un componente antivirus Internet que intercepte y bloquee las secuencias de comandos (scripts) de los sitios web que supongan una amenaza. Todo el tráfico HTTP debe de ser sometido también a un control avanzado.
- Debe contar con la opción de corroborar los vínculos de internet y compararlos con una base de datos web sospechosos y así evitar el “phishing”.
- Debe contar con un componente de prevención de ataques de programas maliciosos para detectar la realización de operaciones que puedan dañar la información antes de su ejecución.
- Debe poder tomar decisiones para el manejo de aplicaciones potencialmente peligrosas.
- Debe contar con un componente que sea capaz de rastrear publicidades no autorizadas (inserciones publicitarias, ventanas independientes).
- Debe proteger los equipos mientras están conectados a Internet u otras redes, debe supervisar las conexiones entrantes y salientes, además de explorar los puertos y los paquetes de datos.
- Debe analizar archivos y enlaces transferidos vía los servicios de mensajería instantánea más comunes como ICQ y Windows Live Messenger
- Debe contar con un componente para supervisar el acceso de los usuarios a dispositivos externos instalados en el equipo. Debe ser capaz de limitar el acceso de la aplicación a dispositivos del USB.
- Debe contar con un módulo de Firewall que sea capaz de realizar filtrado de paquetes y filtrado de aplicaciones.
- El módulo de Firewall del antivirus debe permitir autorizar y bloquear aplicaciones y paquetes de red.
- El módulo de Firewall del antivirus debe contar con la posibilidad de volver al equipo en Modo invisible, para impedir que el equipo pueda ser detectado desde el exterior.
- El módulo del Firewall del antivirus debe contar con reglas para

aplicaciones y para filtrado de paquetes de datos actualizables mediante los archivos de actualización (updates) del fabricante.

- El módulo del Firewall del antivirus debe contar con un sistema de detección de intrusiones cuya base de datos de ataques de red sea actualizable mediante los archivos de actualización (updates) del fabricante.
- El módulo del Firewall del antivirus debe contar con cuatro niveles de protección. Estos niveles serán:
    1. Seguridad máxima
    2. Aprendizaje
    3. Seguridad baja
    4. Autorizar todo

- El cambio de niveles de seguridad debe realizarse de manera local y de manera centralizada por el servidor de administración.
- El módulo de Firewall del antivirus debe ser capaz de exportar e importar las reglas de filtrado de paquetes y de aplicaciones.
- El módulo de Firewall del antivirus debe contar con zonas de seguridad para Internet, Red local y para conexiones de total confianza.
- El módulo de Firewall del antivirus debe contar con un monitor de red que proporcione información detallada acerca de todas las conexiones establecidas en el equipo, los puertos abiertos y el volumen de tráfico entrante y saliente.

B. Para Windows Server el antivirus:

- Debe ser capaz de escanear todos los archivos que son ejecutados, abiertos y/o modificados y desinfectar o eliminar todos los archivos infectados.
- Los archivos o los contenidos sospechosos deben ser aislados en un área de cuarentena antes de someterlos a un análisis más profundo.
- Debe ser capaz de realizar escaneos de áreas específicas del sistema de acuerdo con un horario o bajo demanda.
- Debe escanear aquellas áreas críticas del sistema operativo que son más susceptibles de infección, como una tarea por separado.
- Debe registrar cualquier ataque de malware
- Debe recuperar el sistema después de la infección eliminando todos los registros creados por el programa malicioso en los archivos del sistema o en el registro del sistema.
- Debe ser capaz de escanear totalmente los archivos del sistema, pero contar con una tecnología que solamente revise los archivos nuevos o modificados en los escaneos bajo demanda subsecuentes.
- Debe permitir excluir procesos seguros de ser escaneados.
- Todas las características del antivirus de servidores de archivos deben ser administradas desde una consola central.
- Debe ser capaz de optimizar la utilización de recursos del sistema compartidos con otras aplicaciones según las prioridades de las tareas en ejecución.
- Debe ser capaz de realizar análisis en segundo plano.

C. Para Linux el antivirus debe contar con al menos las siguientes características:

- Debe ser administrable desde un servidor central

- Debe interceptar las solicitudes del sistema de archivos, escanear los archivos que están siendo accedidos por códigos maliciosos, limpiarlos o eliminar los objetos infectados, o bien aislar los objetos sospechosos para un análisis más minucioso.
- Debe ser capaz de escanear áreas específicas buscando objetos infectados y sospechosos de manera programada o a solicitud del administrador de la solución antivirus.
- Debe poder realizar distintas operaciones al encontrar archivos infectados para su manejo, entre otras: desinfectar, eliminar o aislar para un análisis más minucioso.
- Los objetos infectados, sospechosos y dañados que se detectan en un servidor Linux deben poder ser movidos a una carpeta de cuarentena, donde a estos, puedan realizarse distintas operaciones de desinfección y análisis.
- Debe incorporar el soporte para salvar copias de objetos infectados, antes que sean tratados, haciendo posible utilizar las copias para restaurar el archivo original en caso de que resulten dañados.
- El antivirus debe poder ser configurado vía el archivo de configuración de la aplicación o centralmente utilizando el servidor central de administración.
- Para servidores Linux el antivirus debe poder ser configurado, además de las opciones anteriores, vía internet.

17.1.8. Consola de administración central

- Debe contar con procedimientos para generar scripts de desinstalación de otros antivirus.
- Debe administrar el tráfico durante la instalación.
- Debe poder crear paquetes autoinstalables.
- Debe ser capaz de generar reportes exhaustivos sobre el estatus de protección de la red en formato HTML u otros.
- Debe tener soporte para SNMP.
- Deberá contar con una desinstalación automatizada de otros antivirus.
- Mostar los tableros que despliegan el estatus actual de la protección anti-virus en la red
- Capacidad de integrarse con el Directorio Activo de Microsoft para la aplicación de políticas.
- A través de la consola se podrá obtener las características del HW, SW y los procesos que están corriendo en una determinada estación de trabajo
- Debe poder ser instalado con todos sus componentes en sistemas operativos Windows y Windows Server.
- Debe Administrar los productos antivirus para estaciones de trabajo Windows Linux y Mac, así como para servidores de archivos Windows Server y Linux.
- Debe poder instalar de manera remota los productos antivirus para estaciones de trabajo y servidores de archivos (Windows)
- Debe poder realizar la actualización de las definiciones de firmas de antivirus a todos los productos administrados.
- Debe operar de forma remota el monitoreo y mantenimiento del sistema sin interferir las actividades de los usuarios.
- Debe realizar las operaciones de instalación y configuración del producto antivirus sin notificaciones al usuario o solicitudes de interacción al usuario.
- Debe ser capaz de controlar los productos de seguridad de plataformas móviles (Windows Mobile y Symbian).
- Debe realizar descarga centralizada de actualizaciones de datos y módulos que requiera el antivirus.

- Debe distribuir las actualizaciones de datos y módulos que requiera el antivirus de manera automática o manual a través de la red local.
- Debe permitir la personalización del modo de operación conforme a las características de los usuarios de la consola de administración.
- Debe permitir adecuar las características de su interfaz de acuerdo al perfil de cada usuario.
- Debe tener la capacidad de configurarse para formar grupos de usuarios y aplicar distintas directivas y/o políticas a cada grupo de usuarios.
- Deberá ser capaz de notificar los eventos de virus.
- deberá tener la capacidad de registrar todos los eventos contra de vulnerabilidad de la seguridad generados en las estaciones de trabajo como detección y limpieza de malware, spyware, adware, detección de intrusos, intentos de desactivación del software de seguridad; ya sea por el usuario o por código malicioso.
- Debe poder almacenar un histórico de eventos por cada equipo administrado.
- Capacidad de gestionar y conformar a grupos de usuarios, permitiendo administrar desde un solo sólo punto o consola la totalidad de equipos del Ministerio de Educación.

17.1.8.1. Instalación del Producto en las Estaciones de Trabajo.

El producto a ofertar debe tener total compatibilidad con Microsoft Installer. La instalación del producto o su agente en los equpos de los usuarios deberá ser mediante la consola de Administración (Instalación desatendida), propietaria del fabricante del producto a ofertar y/o mediante medio magnético, y/o instalación manual (Instalación personalizada).

17.1.8.2. Políticas

- Las políticas que están implementadas en el MED, deberán implementarse en la solución ofertada, las mismas que deberán ser coordinadas con la Oficina de Informática como ente regulador.

- El producto debe contar con sus propias medidas de seguridad, en este sentido debe ser capaz de no dejar que el usuario pueda desinstalar o bloquear la solución.

- El producto a ofertar no debe permitir que el usuario pueda configurar la solución de manera distinta a la establecida por la política general del Ministerio de Educación.

17.1.8.3. Alertas y Reportes.

- Deberá generar reportes gráficos del tipo barra, pastel, que sean imprimibles y exportables a formato Excel de la cobertura efectuada.

- Deberá generar reportes sobre el estado de la red en línea, debiendo mostrar en tiempo real lo que está ocurriendo.

- Deberá generar alertas de virus mediante correo electrónico y/o alerta de registro entre otros.

17.1.8.4. Adicionalmente.

- El proveedor deberá entregar 03 licencias de antivirus de producto nacional, las que se utilizará como una herramienta de apoyo para el personal de soporte técnico, en el caso de presentar alguna anomalía en las estaciones de trabajos, producido por un malware, este antivirus adicional minimizara el riesgo de haber sido infectado por algún otro virus que no contenga dentro de su lista del principal solicitado:

  - ✓ Detecta y elimina malwares (softwares maliciosos: virus, troyanos, gusanos, rootkits, spywares, adwares, backdoors, botnets, keyloggers) sin necesidad de interrumpir la actividad del usuario y "aplicaciones no deseadas" (AD-WARES, SPY-WARES, DIALERS)
  - ✓ Actualizaciones Inteligentes.
  - ✓ Reinstalación del antivirus cuantas veces sea necesario.
  - ✓ Trabaja con todos los sistemas operativos para estaciones y servidores:
  - ✓ Estaciones: 2000 / NT / 98 /XP/ Vista/Seven
  - ✓ Servidores: Windows 2008/2003/2000 Server /Linux
  - ✓ Protección en Tiempo Real y en línea

17.1.9. Control de Acceso a la Red (Network Access Control).

- El producto a ofertarse debe integrarse con el actual sistema de Control de Acceso a la Red (Network Access Control), inclusive tiene que tener una interacción con el Directorio Activo y con los servicios Windows de LDAP para poder establecer políticas de control de acceso a la Red interna del Ministerio de Educación.
- Por lo tanto, esta integración es de gran utilidad que el sistema NAC se integre con la herramienta de seguridad, específicamente el antivirus que el proveedor ofertará.
- Así mismo el Control de Acceso a la Red (Network Access Control) del Ministerio de Educación, está basado en un servidor Tacacs+ y las herramientas como: Syslog- Server, Nesus, Netflow, snmp y cisco Works.

17.1.10. Despliegue.

- La totalidad de equipos a implementar será un plazo no mayor a 60 días calendarios de la fecha de firma del contrato, se precisa que este servicio incluye la instalación, soporte y configuración de la solución de Antivirus con la última versión, en todos los equipos de la sede del MED señalaos en el cuadro Nº 01.
- El proveedor deberá dejar instalado, configurado, actualizado (de ser necesario el proveedor deberá actualizar el Sistema Operativo) y en optimo funcionamiento.
- El proveedor deberá realizar la instalación, configuración, scaneo, limpiado y una capacitación personalizada en el usos de cómo scanear y eliminar.
- El Proveedor reportara diariamente las instalaciones efectuadas, las cuales deberán estar validadas en la consola del WSUS y Administración del Antivirus.
- Asimismo deberá llenar la ficha técnica de conformidad del usuario.
- El proveedor contara con las facilidades necesarias y el apoyo a todo nivel para no retrasar la instalación.
- El producto deberá incorporar un sistema de eliminación de software antivirus de terceros, que permita desinstalar el producto anteriormente instalado e instalarse sin requerir de procesos manuales, con la finalidad de optimizar el proceso de despliegue de la solución, este sistema debe ser propietario del fabricante
- Además el proveedor deberá asumir de forma conjunta y como una solución integral todas las licencias sin costo alguno para el MED incluyendo todas las versiones hasta el término del contrato.
- El proveedor deberá ofrecer y mantener un sitio WEB para que se pueda bajar e instalar el antivirus en las estaciones de trabajo del MED.

17.1.11. Equipo y Software.

- El Postor que ofrezca el antivirus y filtrado de contenido, deberá ofrecer los equipos necesarios lo suficientemente robustos, de tal manera que garanticen el optimo funcionamiento y operación del sistema solicitado, en alta disponibilidad.
- Este equipo siempre dispondrá del 30% de capacidad libre promedio mensual de los recursos de almacenamiento, memoria RAM, procesador, si este no cumpliera el proveedor tendrá que aumentar la capacidad solicitada.
- La solución a entregarse deberá tener incluido una herramienta que mida los recursos utilizados y el porcentaje.

17.1.12. Idiomas Admitidos.

La solución en cada estación de trabajo del usuario final de la institución deberá de estar configurada e instalada en el idioma Español, dado que este es un producto de usuario final, no se aceptará en ningún otro idioma, sin embargo puede contener aparte del español otros idiomas.

17.2. PRODUCTO 02 – FILTRADO DE CONTENIDOS Y ANTISPAM

CANTIDAD A ADQUIRIR: 2,000 Licencia

El producto a ofertar deberá tener un sistema que permita controlar y bloquear el uso de programas y aplicaciones que desde Internet saturan el ancho de banda y provocan el incumplimiento de las políticas de navegación por Internet del Ministerio de Educación, este sistema debe ser propietario del fabricante y deberá actualizar sus categorías en forma automática y a la hora que se configure (sin intervención del administrador del sistema de la solución), con las siguientes características:

17.2.1. Funcionamiento.

- Centralizado, a nivel de servidores Proxy.
- Permitir el establecimiento de una conexión desde cada sede hacia el servicio de filtrado de contenidos, considerando cada sede como una licencia, independientemente del número de computadoras totales atendidas detrás de cada servidor Proxy.
- Permitir el establecimiento de una conexión desde las estaciones de trabajo del Ministerio de Educación.
- En caso de sobre carga este balanceara la carga entre los equipos.
- El equipo deberá trabajar en alta disponibilidad.

17.2.2. Licencias

Cada vez que se haga referencia a “licencia” se entenderá como un host o una sede que usará de manera licenciada (formal) el servicio de filtrado de contenido web.

Toda licencia o suscripción de software que sea requerida por la solución deberá estar cubierta por el proveedor por el tiempo ofertado y estar licenciado hasta la última versión, sin incurrir costo y gasto alguno para Ministerio de Educación, así como la instalación de sus últimas de versiones.

17.2.3. Forma de integración

La solución ofrecida debe permitir integrarse a nuestros sistemas por Modo bridge y/o proxy y/o en forma transparente u otra forma sin que este baje la performance de la red y del sistema. El modo bridge permite tener dos conexiones de red que reciben y entregan el tráfico de modo full duplex (dos puertos reciben y analizan el trafico). Por lo que el flujo del tráfico sobre la utilización de ambos puertos se realiza al 100%. Al ser modo bridge permite que se incorpore de manera sencilla en cualquier nodo de la red, sin tener grandes intervenciones en la misma. Debe tener una interface de red para acceder a supervisión y monitoreo.

17.2.4. Trazas de filtrado

Búsqueda en base de datos local, análisis de contenido y URL.

17.2.5. Actualización de trazas

Automática, vía http/ftp, con capacidad de poder programar el horario de actualización. Las actualizaciones deberán ser en forma continua e incremental durante la vigencia del contrato.

17.2.6. Especialización

- La plataforma debe permitir la creación de usuarios administradores (mínimo 500 administradores) con el objetivo de que cada sede tenga la posibilidad de administrar sus políticas de filtrado, sin desnaturalizar la política general.

- El postor deberá proveer información de dominio público que sustente el cumplimiento de lo solicitado.

17.2.7. Actualización del software

- Deberá ofrecerse actualización automática del software (motor de filtrado y/o interfase Web) durante el período de vigencia del contrato.
- La actualización del software deberá ser previamente coordinado con personal técnico de la OFIN

17.2.8. Tipos de filtrado

- URLs, incluido el trafico web cifrado (HTTPS,SSL,TLS,etc)
- Palabras claves
- Spyware
- Malware
- FakeAV
- Phishing
- Código malicioso (VBS, Java Script)
- MP3
- Ejecutables (*.exe)
- P2P (peer to peer)
- Banners
- Layers
- Virus
- Proxys Anónimos y Proxys Públicos.
- Filtrado de sitios web que despliegan zombies (BOT Networks), que utilizan las redes internas para denegación del servicio (DoS), robo de identidad, robo de información, etc.
- El bloqueo del tráfico conforme al tipo de protocolo y/o puerto en el que se establece la comunicación (Mensajería Instantánea, Chat, Peer to Peer, etc) pudiendo configurarse en virtud de lo solicitado por el usuario final, atendiendo a sus necesidades específicas.

17.2.9. Filtrado

Multilenguaje, debe ser capaz de utilizar algoritmos para el discernimiento de contenido y técnicas de aprendizaje continuo para detectar contenido inadecuado.

17.2.10. Concurrencia de usuarios

Que soporte al menos 50,000 conexiones concurrentes http, actualmente el Ministerio de Educación cuenta con un servicio de internet de 80 Mbps y 30 Mbps en al WAN, en algunos casos el MED aumenta el ancho de banda (160 Mbps – Internet y 80 Mbps – WAN), este debe soportar sin presentar latencia a la red ni limitaciones para el filtrado y la navegación.

17.2.11. Manejo de listas

- El sistema debe de manejar un sistema de listas Blancas y Listas Negras, debe de existir una prioridad de filtrado de las bases de datos de listas y deberá ser como sigue:
    - Listas del fabricante Generales: Bases de listas del fabricante, son las que tienen el nivel más bajo de prioridad.
    - Listas de la OFIN: Administradas por el personal del centro de datos del la OFIN, prevalecen sobre las listas generales.
    - Listas de la sede: Tienen la prioridad administradas por el personal de cada sede, No prevalecen sobre las listas generales y de la OFIN.

17.2.12. Contención de abusos

Configurar el bloqueo de IP de origen por intentos repetidos de acceso a páginas web restringidas, y generar las alertas correspondientes para la identificación y toma de medidas correctivas, este punto es opcional.

17.2.13. Sistemas operativos

Debe operar y soportar de modo nativo sobre los sistemas operativos:
Windows 2000/2003/2008 Server, Linux (Kernel 2.6).
Toda licencia o suscripción de software que sea requerida por la solución deberá estar cubierta por el proveedor por el tiempo ofertado y estar licenciado, sin incurrir costo y gasto alguno para Ministerio de Educación.

17.2.14. Categorización

Deben soportar categorización (pornografía, violencia, racismo, apuestas en línea, hacking, cracking, etc.) El filtro debe de tener al menos 40 categorías de filtrado de fábrica y debe permitir el reporte a fábrica de sitios no filtrados o filtrados inadecuadamente (falsos positivos), para su incorporación y/o corrección en futuras actualizaciones.

17.2.15. Certificaciones del Producto.

El producto a ofertar debe estar incluido en el cuadrante mágico de Gartner de plataformas de protección de WEB.

17.2.16. Actualizaciones URL y Software.

Se denomina Actualización URL y Software al paquete de datos que se actualiza desde Internet hacia la solución instalada localmente; en este sentido la actualización constante del producto con el nuevo release o última actualización disponible en el mercado, durante el periodo de vigencia del contrato, permitirá una adecuada protección de la Red Informática Interna del Ministerio de educación.

17.2.17. Personalización

Debe permitir la construcción de grupos y categorías de usuarios, de modo de elevar o disminuir la sensibilidad de filtrado.

17.2.18. Políticas.

Las políticas que están implementadas en el MED, y que deberán implementarse en la solución que se pretende adquirir, deberán ser

coordinadas con la Oficina de Informática como ente regulador y el postor como la empresa que implementará la solución.
El producto debe contar con sus medidas propias de seguridad, en este sentido debe ser capaz de no dejar que el usuario pueda desinstalar o bloquear la solución.

17.2.19. Manuales de ayuda del producto

Debe de proporcionar un manual de ayuda para todos los usuarios del sistema (administradores de consola), en el que se explica detalladamente el funcionamiento de cada una de las opciones del interfaz de administración. Así mismo, en cada una de las pantallas del servicio, deben de existir leyendas que ayudan y guían al usuario en cada momento.

17.2.20. Excepciones

Debe permitir el acceso especial a sitios bloqueados por defecto mediante la identificación del usuario (nombre y clave), para efectos de verificación y confirmación o descarte de la regla de filtrado y bloqueo.

17.2.21. Administración

Debe permitir la administración centralizada mediante una interfase Web.

17.2.22. Idioma (interfase)

Español.

17.2.23. Idioma (filtrado)

Filtrar los principales idiomas utilizados en Internet con una eficacia superior al 95%, de la cuales sitios en inglés, castellano, francés, alemán China, Rusia, Ucrania y entre otros.

17.2.24. Localización

El proveedor deberá categorizar y configurar la solución para que permita el acceso a:

- Medios de prensa peruanos
- Instituciones Financieras (Bancos, etc.)
- Instituciones del estado (dominios *.gob.pe)
- Instituciones educativas (dominios *.edu.pe)
- Organizaciones en general (dominios *.org.pe,*.com.pe)
- Dominios de segundo orden (Dominios *.pe)
- Categorización e incorporación, dentro de las 12 horas, de direcciones web reportadas por el personal técnico del Centro de Datos de la OFIN.

17.2.25. Alertas

- Debe proveer alertas personalizadas para el usuario indicándole que la página no ha sido desplegada debido a políticas de filtrado establecidas por la institución.
- Debe permitir configurar el bloqueo IP de Origen y generar las alertas correspondientes.
- Debe permitir la configuración y envío de comunicaciones masivas, a través de mensajes emergentes, permitiendo la programación para que disparé a uno o más host a una determinada hora y/o cuando ingresen a una determinada pagina WEB.
- No se restringe el tipo ni la cantidad de alertas generadas.
- La plataforma debe permitir la configuración de alarmas, para ser enviado a los operados por medio del correo u otro medio.

17.2.26. Reportes

- Debe permitir la emisión de reportes estadísticos que reflejen la operación de filtrado de tiempo real. Independientemente del modelo de comercialización, la oferta deberá incluir el componente de generación y despliegue de reportes.
- Los reportes serán generados por los administradores del Centro de Datos de la OFIN. Sistema de registros e índices compactados que realiza búsquedas sobre los datos disponibles de forma rápida y eficiente, minimizando el uso del espacio en el disco y servidores adicionales a utilizar.
- Los reportes generados pueden ser visualizados a través de formatos html, pdf, y csv.
- Deberá generar reportes sobre el estado de la red en línea, debiendo mostrar en tiempo real lo que está ocurriendo.
- Deberá emitir reportes que contengan:
  - .• Intentos de violación a las políticas del sistema
  - .• Horas que el usuario permanece conectado.
  - .• Ancho de banda usado.
  - .• Sitios visitados.

17.2.27. Protección de correo electrónico (Antispam).

- Creación de políticas para correos entrantes y salientes, listas blancas y negras de modo personal o global, reportes, sistema de solicitud de soporte, cuarentenas, etc.
- Filtrado de correos de entrada y salida en modo transparente
- La solución para el Gateway de correo deberá incluir el soporte para sistemas de archivamiento de correo..
- La solución para el Gateway deberá incluir la capacidad para instalar el producto en modo de alta-disponibilidad los cuales deberán ser administrados desde una única consola de administración.
- Deberá integrarse con los servicios de directorio de Microsoft, Lotus Domino y LDAP para la autenticación de usuarios y creación de políticas.
- Deberá incluir un filtro Anti Spam que soporte descargas automáticas de políticas anti Spam.
- Deberá incluir varias técnicas de detección, como reputación de IP, heurística avanzada, huellas de mensajes y adjuntos, análisis de palabras claves, detección de direcciones web, etc.
- Permitir configurar la detección sobre todos los archivos, o tipos de archivos, comprimidos (cualquier formato de compresión, rar, zip, cab, arj, arz), ocultos y archivos en ejecución.
- El producto debe tener una efectividad de detección de SPAM con un mínimo del 98% de efectividad, para comprobar esta funcionalidad el postor deberá entregar información del fabricante del producto o declaración jurada.
- Deberá detectar ataques de robo de información (phishing) y ataques de denegación de servicio (DoS).
- Deberá contar con un módulo específico para el Filtrado por Reputación que permite el bloqueo por IP's de servidores de dudosa procedencia y permitir elaborar excepciones tanto a nivel MTA como a nivel de políticas de correo. Esta lista deberá residir en el servidor y deberá ser actualizado en promedio cada 15 minutos y en forma incremental.
- Deberá soportar el sistema SPF (Sender Policy Framework) para evitar entrada de correo falsificado, así como también, deberá soportar el sistema de autenticación de correos conocido como DomainKeys.

- Deberá de poder detectar, eliminar virus y spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje.
- Deberá de realizar el bloqueo de archivos adjuntos según el tipo de extensión.
- Deberá de realizar el bloqueo de correos por asuntos, destinatario o texto en el cuerpo del mensaje.
- Deberá contar con un Editor de Políticas para filtrar el contenido del tráfico entrante y saliente.
- Deberá de poder hacer creaciones de lista de aceptación y negación (blanca y negra) de dominios y usuarios (cuentas de correo) confiables.
- Deberá enviar notificaciones configurables al emisor, receptor y al administrador sobre mensajes electrónicos infectados y/o bloqueados.
- Debe permitir crear usuarios para la administración basada en roles para delegar ciertas funcionalidades de administración.
- El acceso a la interfaz de administración basada en roles debe ser vía web seguro
- Deberá contar con un administrador de cuarentena central a nivel de consola.
- Deberá contar con un sistema administrador de la cuarentena por usuario que permita a su vez administrar la lista blanca y negra de cada usuario.
- Debe poder desactivarse en ciertas opciones a las cuales se desea que los usuarios Administradores no tengan acceso.
- Deberá contar con un sistema automático que permita realizar el Backup de la cuarentena. Esta opción es configurable desde la herramienta de gestión del producto.
- La herramienta debe contar con un sistema de actualización de cada parte de los componentes del producto incorporado en la herramienta de administración web.
- No deberá requerirse la instalación de scripts ni productos de terceros para el funcionamiento del producto.
- Deberá de rastrear, eliminar virus adware, spyware y códigos maliciosos en los protocolos SMTP y Gateway
- El postor deberá incluir en su propuesta la protección de los servidores de correo tanto en plataforma Linux, Windows y Lotus Domino.
- Deberá contar con un sistema de administración segura vía Web (http).
- Deberá de incluir un filtro Anti Spam centralizado que soporte descargas automáticas de políticas Anti Spam.

A. Funcionalidades del Antispam

Permitir parametrizar y configurar la solución de antispam teniendo en cuenta las siguientes funcionalidades:

- Permitir activar o desactivar la política de filtrado de spam.
- Permitir crear y editar una política antes de activarla.
- Permitir configurar el Origen y Destino en cuanto a: El conjunto de usuarios, grupos, IP, etc a los que va a afectar una política.
- Permitir el manejo de Perfiles: la solución debe permitir crear, editar y borrar los perfiles usados para definir las políticas de Antispam de Salida. Cada perfil debe estar compuesto por un conjunto de condiciones como: protocolo, spam, remitente, destinatario, adjuntos o avanzado.
- Permitir frente a una política:
  - ✓ **Borrar**: Descartar el mensaje.
  - ✓ **Permitir**: Dejar que el mensaje alcance su destino.
  - ✓ **Cuarentena**: Enviar el mensaje a cuarentena.
  - ✓ **Etiquetar** Mensaje: Añadir una etiqueta al mensaje como prefijo en el asunto, reemplazando al asunto, en el cuerpo del mensaje o reemplazando el mensaje por la etiqueta y añadiendo el mensaje como archivo adjunto.
  - ✓ **Redirigir**: Desviar el mensaje a una nueva dirección de email.
  - ✓ **Copia** a: Entregar el mensaje original al destinatario y enviar una copia a una nueva dirección de email.
  - ✓ **Añadir** remitente a una lista de IPs/Clientes Comprometidos: Esta acción no debe afecta directamente al email recibido. Añadir la dirección IP del remitente y el ID del cliente a una lista de IPs/Clientes potencialmente comprometidos. Esta lista debe ser entonces incluida en un perfil y ser usada en una nueva política para definir una acción global sobre IPs/Clientes comprometidos.
  - ✓ **Quitar** remitente a la lista de IPs/Clientes Comprometidos: Esta acción no debe afectar directamente al email recibido. Eliminar la IP de un remitente y el ID del cliente de la lista de IPs/Clientes potencialmente comprometidos.
  - ✓ **Rechazar**: Esta acción debe rechazar los emails salientes y envía un código de error al remitente original.
  - ✓ **Horario:** Esta opción debe permitir definir el lapso de tiempo en el que se aplicará la política.

B. Cuarentena

- La solución debe proveer un módulo de Cuarentena que se utilice para almacenar, mostrar y desbloquear los mensajes que han sido identificados como spam y enviados a la Cuarentena por las políticas de filtrado.
- Los mensajes de email en cuarentena se deben mostrar en pantalla para que el administrador tenga la opción de marcar los mensajes como NO spam, desbloquearlos o borrarlos y vaciar la bandeja de cuarentena.
- Ofrecer mecanismo para busqueda de mensajes usando diferentes criterios de selección.

C. Informes

La solución de antispam debe ofrecer los siguientes informes:

- Informes de servicio que permitan configurar las preferencias momento degenerar los informes de los mensajes recibidos y/o enviados por los clientes, indicando si estos mensajes son considerados o no como spam. Se pueden establecer diferentes parámetros para crear el informe como: id del cliente, dominio, IP origen, remitente, fechas, rangos de tiempo y filtros para agrupar las salidas del informe.
- Informes de monitoreo que le permitan al administrador crear informes detallados sobre la historia del cliente. Estos informes deben mostrar las estadísticas de filtrado de la actividad del cliente con los mismos parámetros que el anterior.

D. Administración de IPS´s comprometidas

La solución debe incluir la posibilidad de administrar la configuración y comportamiento del filtro de spam y manejar la lista de Clientes/IPs Comprometidas.

E. Técnicas de detección de spam

La solución de antispam debe permitir activar diferentes métodos de detección de spam. Estos métodos deben permitirse activar y desactivar al administrador cuando se creen perfiles. De igual forma se debe permitir definir el tamaño máximo aceptado por esta solución para los mensajes. Los mensajes con un tamaño superior deben automáticamente descartarse por la solución. Adicionalmente, permitir especificar el tamaño máximo de un mensaje de spam. Esto significa que cualquier mensaje con un tamaño superior es éste NO será analizado con estos métodos de detección de spam, en otras palabras no pasara, por lo menos los siguientes métodos de detección de spam:

- ✓ Base de datos de confianza.
- ✓ Base de datos contextual de confianza.
- ✓ Catálogo de programas que permiten el envío masivo de mensajes, es opcional.
- ✓ Base de datos externa de confianza.
- ✓ Detección de direcciones simuladas (SPF).
- ✓ Listas cooperativa de direcciones simuladas (DNSBL).
- ✓ Listas grises, es opcional.
- ✓ Comprobación de enlaces URI en bases de datos de categorías.
- ✓ Análisis de contenido de los mensajes de correo electrónico.
- ✓ Análisis semántico de los enlaces URI.
- ✓ Análisis de contenido de los enlaces URI.
- ✓ Comprobación privada de la firma digital de los mensajes de correo electrónico, es opcional.
- ✓ Comprobación cooperativa de firmas digitales conocidas de envío mensajes de correo electrónico no deseado (con firmas para mutaciones básicas), es opcional.

F. GESTION DE EVENTOS:

La solución debe permitir la generación de eventos de la operación de la misma y generar ciertos mensajes con el fin de ayudar al administrador para detectar un problema o una configuración inadecuada.

17.3. Instalación y operación

- La instalación y configuración inicial correrá a cargo del proveedor.
- El postor debe ofrecer lo necesario como parte del bien (no Appliance) el equipo lo suficientemente robustos para la instalación de la solución, de tal manera que garanticen el buen y optimo funcionamiento de la solución en alta disponibilidad.
- Deberán configurarse en modo "clúster" y con operaciones de balanceo de carga. El servicio no debe de ocasionar latencia en la red.
- La solución de filtrado debe ser capaz de funcionar normalmente si es que un servidor falla.

17.4. Plataforma

Dos equipos, como mínimo:

- ✓ Con fuentes de poder redundante
- ✓ Un DVD –RW interno.
- ✓ Discos extraíbles en caliente
- ✓ Cuatro discos SAS 2.5 de 300 GB por disco.
- ✓ Arreglo de disco en 5 + Hot Spare
- ✓ Los servidores trabajaran en un esquema de alta disponibilidad
- ✓ Gestión remota del hardware.
- ✓ Tipo rack de una UR
- ✓ 32 GB de memoria RAM DDR 3 ECC por equipo.
- ✓ Tecnología basada en CORE (04 core)
- ✓ 2.93 GT de velocidad de procesador
- ✓ Memoria cache de 16MB.
- ✓ Dos puerto de red 10/100/1000 Mbps
- ✓ Un monitor de 50" – LED de pared, con los accesorios.
- ✓ Deberán conectarse con cable HDMI de 10mt al monitor.
- ✓ El equipo deberá estar instalado con el S.O. para su correcta operación.
- ✓ Software de administración de la misma marca del equipo del hardware.
- ✓ Software de configuración
- ✓ Análisis predictivo de fallas.
- ✓ Protección de memoria avanzada ECC
- ✓ Sistema ASR (automatic Server Recovery) o similar
- ✓ Sistema RBSU (ROM Based Setup Utility) o similar
- ✓ Equipo certificado en Red Hat Linux y Windows Server 2008.

CAPÍTULO IV

CRITERIOS DE EVALUACIÓN

PRIMERA ETAPA: EVALUACIÓN TÉCNICA
(Puntaje Máximo: 100 Puntos)

1. EXPERIENCIA DEL POSTOR 40 PUNTOS

La experiencia del postor será calificada **considerando la venta de software antivirus Y SIMILARES (*).** Asimismo, dicha experiencia será acreditada a través de la presentación de **contratos y/u órdenes de compra** y la respectiva conformidad por la venta de los suministros efectuados, o mediante **comprobantes de pago** cuya cancelación se acredite **documental y fehacientemente** (el documento debe presentar sello de pagado o cancelado o adjuntar comprobante o voucher de depósito del pago en Entidad del sistema bancario y financiero nacional), con un máximo de veinte (20) contrataciones, sin importar el número de documentos que las sustenten. En el caso de suministro de bienes, sólo se considerará la parte que haya sido ejecutada hasta la fecha de presentación de propuestas, debiendo adjuntar la conformidad de la misma o acreditar su pago. Los documentos que sustenten la experiencia del postor deben contar con una antigüedad **no mayor a ocho (8) años,** computados hasta la fecha de la presentación de propuestas.

Similares: **software que se dedique a evitar ataques y restricciones informáticos entre ellos: antimalware, filtrado de contenido, IPS/IDS y antispam.**

Asimismo, los postores deberán llenar el formato del **Anexo Nº 05.** No se considerarán aquellos comprobantes de pago, contratos, órdenes de compra ni conformidades ilegibles que presenten borrones o enmendaduras o, que presenten información incompleta o con errores.

La puntuación será otorgada conforme al siguiente detalle:

Monto de Facturación	Puntaje
Monto igual o mayor a 2 veces el valor referencial	40 PUNTOS
Monto igual o mayor a 1 vez el valor referencial y menor a 2 veces el valor referencial	30 PUNTOS
Monto menor a 1 vez el valor referencial	00 PUNTOS

En las copias de los comprobantes de pago, contratos u órdenes de compra presentados, cuyo monto se consigne en dólares u otra moneda, el postor deberá indicar el tipo de cambio utilizado en la fecha de emisión de los comprobantes de pago, elaboración del contrato u orden de compra. Caso contrario, se considerará el tipo de cambio a la fecha de evaluación de propuestas.

Nota:

a) El consorcio que se presente como postor al proceso de selección deberá de acreditar su experiencia sumando los montos facturados de aquellas empresas consorciadas que se hubieran comprometido a ejecutar conjuntamente el objeto materia de la convocatoria.
b) En el caso de la adquisición de éste tipo de bienes, cuya entrega se haya efectuado en forma periódica, sólo se considerará la parte que efectivamente ejecutada hasta la fecha de presentación de propuestas, debiendo adjuntar la conformidad de la misma o acreditar su pago a través de la factura.

c) En el caso de facturas o contratos donde el postor o alguno de sus consorciados haya participado como parte de un consorcio, únicamente se le considerará como experiencia la parte proporcional atendiendo al número de empresas que lo integran, salvo que el postor adjunte además la copia de la formalización de consorcio correspondiente a dicho servicio donde se indique de modo claro e indubitable cuánto fue su porcentaje de participación.

Asimismo, en los casos de consorcio, solamente será considerada la experiencia de los consorciados que en su Promesa Formal de Consorcio hayan indicado expresamente la venta del bien objeto de la convocatoria, en caso contrario, se considerará que todos los miembros del consorcio lo prestará.

2. MEJORAS RESPECTO A LA SOLUCIÓN 60 PUNTOS

2.1 MESES DE USO DE LICENCIAS ADICIONALES 10 PUNTOS

El postor que ofrezca meses adicionales de uso de licencias y soporte para toda la solución:

Tres meses a más	10 puntos
Dos meses	06 puntos
Un mes	04 puntos

2.2 GARANTÍA DE HARDWARE (SERVIDORES) ADICIONAL 10 PUNTOS

Se otorgará el puntaje al postor que oferte un (1) año de garantía adicional, respecto al hardware (servidores), que incluya mantenimiento preventivo y correctivo.

2.3 LICENCIAS ANTIVIRUS Y FILTRADO DE CONTENIDO ADICIONAL 30 PUNTOS

Se otorgará puntaje al postor que oferte 100 Licencias y Filtrado de contenido adicional.

2.4 FUNCIONALIDADES ADICIONALES 10 PUNTOS

2.4.1 FILTRO DE CONTENIDO Y ANTISPAM
Se otorgará el puntaje al postor que ofrezca: filtro de contenido y antispam administrados desde la misma plataforma y consola.

2.4.2 CONTROL DEL ANCHO DE BANDA
Se otorgará puntaje al postor cuya plataforma de filtrado pueda controlar el ancho de banda por IP.

Para Obtener puntaje en el factor de evaluación Nº 2, deberá presentar la declaración jurada de mejoras, **de acuerdo al ANEXO Nº 7**.

PARA ACCEDER A LA ETAPA DE EVALUACIÓN ECONÓMICA, EL POSTOR DEBERÁ OBTENER UN PUNTAJE TÉCNICO MÍNIMO DE SESENTA (60) PUNTOS.

CAPÍTULO V

PROFORMA DE CONTRATO

LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024

ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIDAS DEL MINISTERIO DE EDUCACIÓN

Conste por el presente documento, la adquisición de antivirus, filtrado de contenidos y antispam para la Sede Central y Sedes descentralizadas del Ministerio de Educación, que celebra de una parte, **EL MINISTERIO DE EDUCACIÓN – UNIDAD EJECUTORA 024**, en adelante **"LA ENTIDAD",** con RUC N° 20131370998, con domicilio legal en la Avenida De la Poesía 155, distrito de San Borja, Provincia y Departamento de Lima, representada por el Secretario General, el Sr. Eco. Asabedo Fernández Carretero, identificado con DNI. N° 08187468, designado mediante Resolución Ministerial Nº 0454-2006-ED de fecha 03 de agosto de 2006 y debidamente facultado por Resolución Ministerial N° 001-2011-ED de fecha 05 de enero de 2011, y de otra parte,…….., con RUC Nº …….., con domicilio legal en……., distrito de…., Provincia…. y departamento de….., inscrita en la Partida Nº ……, Asiento…….del Registro de Personas Jurídicas de la Oficina Registral de……., debidamente representado por su Representante Legal,…….., con DNI N°……., según poder inscrito en la Partida Nº…….., Asiento……..del Registro de Personas Jurídicas de ……., a quien en adelante se le denominará **"EL CONTRATISTA",** en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: OBJETO

Con fecha……..de 2011, el Comité Especial adjudicó la Buena Pro de la **LICITACIÓN PÚBLICACIÓN Nº 006-2011-ED/UE 024** para la adquisición de antivirus, filtrado de contenidos y antispam para la Sede Central y Sedes Descentralizadas del Ministerio de Educación, de acuerdo a sus competencias y responsabilidades, otorgó la Buena Pro a **"EL CONTRATISTA".**

CLÁUSULA SEGUNDA: FINALIDAD DEL CONTRATO

"EL CONTRATISTA" se compromete a entregar los bienes, conforme a las Especificaciones Técnicas contenidos en las Bases de la **LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024** y de acuerdo a su propuesta técnica; que con carácter de Declaración Jurada presentó en su Propuesta Técnica y que forman parte integrante del presente contrato.

DEL SERVICIO DE SOPORTE

Responsable de filtrado de contenido y Antivirus:……, quien cuenta con …(…) certificado en antivirus y…(…) filtrado de contenido, emitidos por el fabricante.

Personal de soporte técnico:……..,……,……, quienes cuentan con …(…) certificados en antivirus y…(…) filtrado de contenido, emitidos por el fabricante.

Coordinador de los proyectos:……., quien estará a cargo de las actividades, cronograma y supervisión.

MODIFICACIÓN DEL PERSONAL

Si el contratista realiza cambios del personal del servicio de soporte, este tendría que ser previamente aprobado por la Oficina de Informática de la Entidad, debiendo ser de la misma o superior a la calidad y experiencia que el personal que ofertó.

CAPACITACIÓN

INSTRUCTORES:…….., quienes cuentan con…(…) certificados en antivirus y…(…) filtrado de contenido, emitidos por el fabricante.

TÉCNICOS DE SOPORTE
Se capacitará a un mínimo de 18 personas, a las cuales se les dará capacitación en dos sub-grupos de 9 personas.

La capacitación se realizará fuera del horario de labores por un período de **ocho (8) horas lectivas**, en los ambientes de la sala de capacitación de la Entidad. La misma tendrá mayor énfasis en los temas de pruebas de despliegue, configuración y resolución de incidentes de la solución.

ESPECIALISTAS
Se capacitará a un mínimo de 15 personas, a las cuales se les dará capacitación en dos sub-grupos.

La capacitación se realizará fuera del horario de labores por un período de **ocho (8) horas lectivas**, en los ambientes proporcionados por el contratista, en el cual deberá ofrecer los equipos necesarios para efectuar capacitación sobre la instalación y manejo de la solución; pruebas de configuración y resolución de incidencias de la solución.

ENTREGA DE CERTIFICADOS
Al finalizar la capacitación, el contratista otorgará a cada participante, un certificado en administración del sistema y soporte técnico en antivirus y filtrado de contenido.

CLÁUSULA TERCERA: PLAZO DE ENTREGA y GARANTÍA

"EL CONTRATISTA" se compromete a entregar la totalidad de los bienes descritos en la cláusula anterior, incluyendo su instalación, configuración y puesta en operación del producto 01 (antivirus) y 03 (filtrado de contenido y antispam) en un plazo no mayor a **sesenta (60) días calendario,** contados **a partir del día siguiente de suscrito el contrato.**

Los bienes adjudicados, serán entregados en el Almacén del Ministerio de Educación, ubicado en Av. Venezuela Nº 1891-Cercado de Lima.

De acuerdo a lo ofertado por el contratista en su propuesta técnica, se otorgará…(…) meses adicionales de uso de licencias y soporte para toda la solución, son costo alguno para la Entidad.

Asimismo, otorga una garantía de…(…) años respecto al hardware (servidores), que incluye el mantenimiento preventivo y correctivo.

De otro lado, el filtro de contenido y antispam serán administrados desde la misma plataforma y consola y se tendrá na plataforma de filtrado que pueda controlar el ancho de banda por IP.

CLÁUSULA CUARTA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a **S/. …….(……con …/100 Nuevos Soles)** a todo costo, incluido IGV.

El monto señalado en el párrafo anterior se desagrega de la siguiente manera:

ITEM	CONCEPTO	UNIDAD	VALOR TOTAL
1	**ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACIÓN**		
1.1	SOFTWARE DE PROTECCION ANTIVIRUS, FILTRADO DE CONTENIDO Y ANTISPAM	1	S/.
1.2	SERVIDORES	2	S/.
TOTAL			**S/.**

Este monto comprende el costo de los bienes, seguros e impuestos, así como todo aquello que sea necesario para la correcta ejecución de la prestación materia del presente contrato.

CLÁUSULA QUINTA: FORMA DE PAGO

"LA ENTIDAD" se obliga a pagar la contraprestación a **"EL CONTRATISTA"** en una sola armada (En Nuevos Soles).

Para el pago, **"EL CONTRATISTA"** deberá presentar ante el Área de Adquisiciones de **"LA ENTIDAD"** la siguiente documentación:

1. Factura por el monto total del contrato.
2. Copia de la Orden de Compra.
3. Conformidad técnica emitida por la Oficina de Informática del MED, señalando el cumplimiento de la prestación, de acuerdo a las especificaciones técnicas de las Bases.
4. Conformidad suscrita por el Jefe del Almacén del Ministerio de Educación.

El pago se efectuará conforme a lo establecido por el artículo 181º del Reglamento.

Durante la vigencia del contrato los precios se mantendrán fijos y no estarán sujetos a reajuste alguno*.*

En el caso de existir observaciones, éstas deberán ser levantadas en un plazo no mayor de cinco (5) días calendarios, debiendo **"LA ENTIDAD"** responder en un plazo prudente. En caso que **"EL CONTRATISTA"** no cumpliese con levantar las observaciones en el plazo establecido, **"LA ENTIDAD"** podrá resolver el contrato.

Así mismo **"EL CONTRATISTA"** señala poseer el Código de Cuenta Interbancario en cuenta de ahorros en nuevos soles Nº ……perteneciente al Banco……ú, para los abonos correspondientes según lo establece la Directiva de Tesorería Nº 001-2007-EF/77.15.

CLÁUSULA SEXTA: VIGENCIA DEL CONTRATO

El presente Contrato tiene vigencia desde el día siguiente de la suscripción del documento que lo contiene, rige hasta que el funcionario competente dé la conformidad de la última prestación a cargo del contratista y se efectúe el pago o hasta su resolución de ser el caso.

CLÁUSULA SÉTIMA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas de la **LICITACIÓN PÚBLICA Nº 006-2011-ED/ UE 024**, la oferta ganadora y los documentos derivados del proceso de selección que establezcan obligaciones para las partes.

CLÁUSULA OCTAVA: GARANTÍAS

EL CONTRATISTA entregó a la suscripción del contrato la respectiva garantía solidaria, irrevocable, incondicional y de realización automática a sólo requerimiento, a favor **de LA ENTIDAD**, por los conceptos, importes y vigencias siguientes:

De fiel cumplimiento del contrato: **……(……..con…/100 Nuevos Soles),** a través de la Carta Fianza Nº ……, cantidad que es equivalente al diez por ciento (10%) del monto del contrato original y tiene una vigencia hasta la conformidad de la recepción de la prestación.

CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD está facultada para ejecutar las garantías cuando **EL CONTRATISTA** no cumpliera con renovarlas, conforme a lo dispuesto por el artículo 164º del Reglamento.

CLÁUSULA DÉCIMA: CONFORMIDAD DE RECEPCIÓN DE LA PRESTACIÓN

La conformidad de recepción de la prestación se regula por lo dispuesto en el Artículo 176º del Reglamento de la Ley de Contrataciones del Estado.

De existir observaciones se consignarán en el acta respectiva, indicándose claramente el sentido de éstas, dándose al contratista un plazo prudencial para su subsanación, en función a la complejidad del bien. Dicho plazo no podrá ser menor de dos (2) ni mayor de diez (10) días calendario. Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la Entidad podrá resolver el contrato, sin perjuicio de aplicar las penalidades que correspondan.

Este procedimiento no será aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la Entidad no efectuará la recepción, debiendo considerarse como no ejecutada la prestación, aplicándose las penalidades que correspondan.

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

El contratista declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad de recepción de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por el artículo 50º de la Ley.

CLÁUSULA DÉCIMO TERCERA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplicará al contratista una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente o, de ser el caso, del ítem que debió ejecutarse en concordancia con el artículo 165° del Reglamento de la Ley de Contrataciones del Estado. En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días.

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

Esta penalidad será deducida de los pagos a cuenta, del pago final o en la liquidación final; o si fuese necesario se cobrará del monto resultante de la ejecución de la garantía de Fiel Cumplimiento.

La justificación por el retraso se sujeta a lo dispuesto por el Código Civil y demás normas concordantes.

CLÁUSULA DÉCIMO CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes podrá resolver el contrato, de conformidad con los artículos 40º, inciso c), y 44º de la Ley, y los artículos 167º y 168º de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 169° del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMO QUINTA: RESPONSABILIDAD DEL CONTRATISTA

Sin perjuicio de la indemnización por daño ulterior, las sanciones administrativas y pecuniarias aplicadas a **EL CONTRATISTA**, no lo eximen de cumplir con las demás obligaciones pactadas ni de las responsabilidades civiles y penales a que hubiere lugar.

CLÁUSULA DÉCIMO SEXTA: MARCO LEGAL DEL CONTRATO

En lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, serán de aplicación las disposiciones pertinentes del Código Civil vigente y demás normas concordantes.

CLÁUSULA DÉCIMO SÉTIMA: SOLUCIÓN DE CONTROVERSIAS

Aplicación de la Conciliación.-
Por la presente cláusula se establece que cualquier controversia sobre la ejecución o interpretación de este Contrato podrá solucionarse por Conciliación.

Cualquiera de las partes tiene el derecho de solicitar una conciliación dentro del plazo de caducidad previsto en los artículos del REGLAMENTO, o, en su defecto, en el artículo 52º de la LEY, debiendo iniciarse este procedimiento ante un Centro de Conciliación acreditado por el Ministerio de Justicia.

Si la conciliación soluciona la controversia en forma total el Acta que contiene el acuerdo es título de ejecución para todos los efectos. Si concluye con un acuerdo parcial o sin acuerdo, las partes deben someterse obligatoriamente a un arbitraje para que se pronuncie definitivamente sobre las diferencias no resueltas dentro del plazo de los quince (15) días hábiles siguientes de la suscripción del acta de no acuerdo total o parcial.

Aplicación del Arbitraje.-
En caso no haya acuerdo para la Conciliación, las partes acuerdan que cualquier controversia que surja desde la celebración del contrato será resuelta mediante arbitraje, conforme a las disposiciones de la LEY y su REGLAMENTO.

El arbitraje será resuelto por un Tribunal Arbitral conformado por tres (3) árbitros. A falta de acuerdo en la designación de los mismos o del Presidente del Tribunal, o ante la rebeldía de una de las partes en cumplir con dicha designación, la misma será efectuada por el Organismo Supervisor de Contrataciones del Estado conforme a las disposiciones administrativas del

REGLAMENTO o conforme al Reglamento del Centro de Arbitraje al que se hubiesen sometido las partes.

El laudo arbitral emitido es vinculante para las partes y pondrá fin al procedimiento de manera definitiva, siendo el laudo inapelable ante el Poder Judicial o ante cualquier instancia administrativa.

El procedimiento de conciliación y arbitraje se ceñirán a lo prescrito en los artículos 214° al 234° del REGLAMENTO.

CLÁUSULA DÉCIMO OCTAVA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes podrá elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA DÉCIMO NOVENA: VERACIDAD DE DOMICILIOS

Las partes señalan como domicilio legal las indicadas en la parte introductoria del presente contrato, lugares donde se les cursará válidamente las notificaciones de Ley.

Los cambios domiciliarios que pudieran ocurrir serán comunicados a **"LA ENTIDAD"** notarialmente y con cinco (5) días de anticipación.

ANEXOS

Forman parte del presente contrato los siguientes documentos:

1. Las Bases Integradas de la **Licitación Pública N°006-2011-ED/UE 024**
2. Propuesta Técnica y Económica de **"EL CONTRATISTA"**
3. La Constancia Nº….del…de….de 2011, emitida por el OSCE de No estar Inhabilitado para contratar con el Estado.
4. Garantía de Fiel Cumplimiento del Contrato
5. Los demás documentos que establezcan obligaciones entre las partes derivados del proceso de selección.

En señal de conformidad con el presente Contrato, las partes lo firman por triplicado en señal de conformidad en la ciudad de Lima el día…de….del año dos mil once.

"LA ENTIDAD" **"EL CONTRATISTA"**

FORMATOS Y ANEXOS

FORMATO N°01

MODELO DE CARTA DE ACREDITACIÓN DEL REPRESENTANTE

Ciudad y fecha, …….

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

……(nombre del postor/ Empresa y/o Consorcio), identificado con RUC Nº …… , debidamente representado por ……. (nombre del representante legal de la persona jurídica), identificado con DNI Nº ……tenemos el agrado de dirigirnos a ustedes, en relación con la **LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024.**, a fin de acreditar a nuestro apoderado: …… (nombre del apoderado) identificado con DNI Nº ……quien se encuentra en virtud a este documento, debidamente autorizado a realizar todos los actos vinculados al proceso de selección.

Para tal efecto, se adjunta copia simple de la ficha registral vigente del suscrito.[16]

……
Firma y sello del representante legal
Nombre / Razón Social del postor

[16] Incluir dicho párrafo sólo en el caso de personas jurídicas y siempre y cuando el Representante Legal de éste no concurra personalmente al proceso de selección, de lo contrario, se procederá de acuerdo a lo dispuesto en el artículo 65º del Reglamento.

ANEXO N°01
DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

El que se suscribe, …… *(o representante Legal de .....)*, identificado con DNI Nº ....., R.U.C. Nº ....., con poder inscrito en la localidad de ..... en la Ficha Nº ..... Asiento Nº ....., **DECLARO BAJO JURAMENTO** que la siguiente información de mi representada se sujeta a la verdad:

Nombre o Razón Social					
Domicilio Legal					
RUC		Teléfono		Fax	

Autorización Municipal

Municipalidad	Nº de Licencia de Funcionamiento	Fecha

Ciudad y fecha, ……

.....
Firma y sello del Representante Legal
Nombre / Razón social del postor

(*) Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados.

ANEXO N°02

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL BIEN CONVOCADO

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

De nuestra consideración:

En calidad de postor, luego de haber examinado los documentos del proceso de la referencia proporcionados por el Ministerio de Educación, y conocer todas las condiciones existentes, el suscrito ofrece entregar los bienes, de conformidad con dichos documentos y de acuerdo con los Requerimientos Técnicos Mínimos y demás condiciones que se indican en el Capítulo III de la sección específica de las Bases.

En ese sentido, me comprometo a entregar el bien con las características, en la forma y plazo especificados en las Bases.

Ciudad y fecha, ……

……..
Firma y sello del representante legal
Nombre / Razón social del postor

(*) Adicionalmente, se acredita los documentos que acreditan el cumplimiento de los Requerimientos Técnicos Mínimos, conforme a lo señalado en el contenido del sobre técnico.

(*) Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados.

ANEXO N°03

DECLARACIÓN JURADA
(ART. 42º DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

De nuestra consideración:

El que suscribe …….. (o representante legal de …….), identificado con DNI Nº ....., con RUC Nº ……, domiciliado en ....., que se presenta como postor del **LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024,** para la **CONTRATACIÓN DE BIENES-ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACIÓN**, declaro bajo juramento:

1.- No tengo impedimento para participar en el proceso de selección ni para contratar con el Estado, conforme al Art. 10º de la Ley de Contrataciones del Estado.

2.- Conozco, acepto y me someto a las Bases, condiciones y procedimientos del proceso de selección.

3.- Soy responsable de la veracidad de los documentos e información que presento a efectos del presente proceso de selección.

4.- Me comprometo a mantener mi oferta durante el proceso de selección y a suscribir el contrato, en caso de resultar favorecido con la Buena Pro.

5.- Conozco las sanciones contenidas en la Ley y su Reglamento, así como en la Ley N° 27444, Ley del Procedimiento Administrativo General.

Ciudad y fecha, ……

……
Firma y sello del representante legal
Nombre / Razón social del postor

(*) Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados.

ANEXO N°04

PROMESA FORMAL DE CONSORCIO
(Sólo para el caso en que un consorcio se presente como postor)

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

De nuestra consideración,

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable durante el lapso que dure el proceso de selección, para presentar una propuesta conjunta en la **LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024** responsabilizándonos solidariamente por todas las acciones y omisiones que provengan del citado proceso.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 141º del Reglamento de la Ley de Contrataciones del Estado.

Designamos al Sr. ....., identificado con D.N.I. Nº…….. como representante legal común del Consorcio, para efectos de participar en todas las etapas del proceso de selección y formalizar la contratación correspondiente. Adicionalmente, fijamos nuestro domicilio legal común en.....

OBLIGACIONES DE ……..: % Participación
-
-

OBLIGACIONES DE ……: % Participación
-
-

Ciudad y fecha, ……

…….
…….
Nombre, firma, sello y DNI del Representante Legal empresa 1

Nombre, firma, sello y DNI del Representante Legal empresa 2

ANEXO N°05

EXPERIENCIA DEL POSTOR

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

El que suscribe....., con (documento de identidad) N°....., Representante Legal de la Empresa....., con RUC. N°....., y con Domicilio Legal en....., detallamos lo siguiente:

Nº	CLIENTE	OBJETO DEL CONTRATO (a)	N° CONTRATO O FACTURA	IMPORTE DEL CONTRATO O FACTURA	FECHA DE INICIO Y TÉRMINO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
TOTAL					

Ciudad y fecha, ……

…….....
Firma y sello del Representante Legal
Nombre / Razón social del postor

ANEXO Nº 06

CARTA DE PROPUESTA ECONÓMICA

Señores
COMITÉ ESPECIAL
LICITACIÓN PÚBLICA Nº 006-2011-ED/UE 024
Presente.-

De nuestra consideración,

A continuación, hacemos de conocimiento que nuestra propuesta económica es la siguiente:

ITEM	CONCEPTO	UNIDAD	VALOR TOTAL
1	**ADQUISICIÓN DE ANTIVIRUS, FILTRADO DE CONTENIDOS Y ANTISPAM PARA LA SEDE CENTRAL Y SEDES DESCENTRALIZADAS DEL MINISTERIO DE EDUCACIÓN**		
1.1	SOFTWARE DE PROTECCION ANTIVIRUS, FILTRADO DE CONTENIDO Y ANTISPAM	1	S/.
1.2	SERVIDORES	2	S/.
TOTAL			**S/.**

La propuesta económica incluye todos los tributos, seguros, transportes, inspecciones, pruebas, y de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que le sea aplicable y que pueda tener incidencia sobre el costo del bien a contratar.

Ciudad y fecha, ……

…….
Firma y sello del representante legal
Nombre / Razón social del postor

ANEXO N° 07

DECLARACION JURADA DE MEJORAS

POSTOR:_____

Dirección:_____

Rep. Legal:_____

D.N.I.:_____ (del representante Legal).

DECLARO BAJO JURAMENTO:

Que nuestra empresa oferta como mejora lo siguiente:

- …(…) meses adicionales de uso de licencias y soporte para toda la solución, son costo alguno para la Entidad.
- …(…) año de garantía adicional respecto al hardware (servidores), que incluye mantenimiento preventivo y correctivo.
- …(…) licencias y filtrado de contenido adicional, sin costo alguno para la Entidad.
- Ofrezca: filtro de contenido y antispam administrados desde la misma plataforma y consola.
- Una plataforma de filtrado que pueda controlar el ancho de banda por IP.

Lima, de del 2011

Atentamente,

(Firma del representante Legal)
(Apellidos y nombres)
(DNI)

Nota: Las cantidades se deberán señalar en números y letras.