BASES

ADQUISICION NIVEL I Nº 003-2017-AGROBANCO

ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB

2017

SECCIÓN GENERAL

DISPOSICIONES COMUNES A TODOS LOS NIVELES DE CONTRATACION

CAPÍTULO I

ETAPAS DE LOS PROCESOS DE SELECCIÓN

Base Legal

- Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros y AFP.
- Ley N° 27603, Ley de Creación del Banco Agropecuario
- Ley N° 29064, Ley de Relanzamiento del Banco Agropecuario
- Ley N° 29523, Ley de Mejora de la Competitividad de las Cajas Municipales de Ahorro y Crédito del Perú
- Ley N° 29596, Ley que viabiliza la ejecución del Programa de Re-estructuración de la deuda agraria (PREDA) y complementarias.
- Directiva de Gestión de las Empresas bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE)
- El Reglamento de Adquisiciones y Contrataciones de AGROBANCO, publicado en la página web de Agrobanco.
- Manual de Procedimientos de Adquisiciones y Contrataciones de AGROBANCO, publicado en la página web del Agrobanco.
- Política de Adquisiciones y Contrataciones de AGROBANCO, publicado en la página web de Agrobanco.

a) De la Convocatoria del proceso de Adquisición

- El Departamento de Logística gestiona la convocatoria del proceso en base al calendario aprobado y realiza la invitación a un mínimo de tres (03) empresas, incluyendo las que participaron en el estudio de mercado.
- La convocatoria de todo proceso de selección se realizará a través de la página web conteniendo la aprobación del expediente, las Bases y la aprobación de las Bases; e invitación directa por correo electrónico a todos los potenciales proveedores de bienes, servicios y obras, adjuntando las Bases.
- Se publicará en la página web las bases del proceso a efecto que el público en general tenga acceso en forma gratuita. Igualmente se registrará el proceso en la web.
- Efectuada la convocatoria, las empresas deberán registrarse obligatoriamente y en forma gratuita, a fin de poder participar en el proceso, adjuntando copia del registro Nacional de Proveedores vigente emitido por la OSCE.

- Los tiempos mínimos para la presentación de las propuestas por parte de los proveedores, se encuentran detallado en el Reglamento de Adquisiciones y Contrataciones de AGROBANCO, tomando en consideración cada nivel de Contratación.

NIVEL	N° de invitaciones	PLAZOS
III Nivel	Mínimo 3.	Desde convocatoria hasta recepción de propuestas: Mínimo 12 días hábiles (*) Desde presentación de propuestas hasta Buena Pro: Mínimo 5 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 8 días hábiles. Desde consentimiento hasta suscripción del contrato: Mínimo 5 días hábiles.
II Nivel	Mínimo 3.	Desde convocatoria hasta recepción de propuestas: Mínimo 9 días hábiles. Desde presentación de propuestas hasta Buena Pro: Mínimo 2 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 2 días hábiles. Desde consentimiento hasta suscripción del contrato: Mínimo 5 días hábiles.
I Nivel	Mínimo 3.	Desde convocatoria hasta recepción de propuestas: Mínimo 2 días hábiles Desde presentación de propuestas hasta Buena Pro: Mínimo 2 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 2 días hábiles. Desde consentimiento hasta la emisión de la orden de compra, servicio o suscripción del contrato: Mínimo 2 días hábiles.

(*) Para las contratación de bienes y servicios cuyos montos fuesen iguales o superiores a US$ 250, 000 o las obras cuyos montos fuesen iguales o superiores a US$ 7 407 000,00, adicionalmente serán de aplicación los TLC suscritos entre el Perú y otro país, por lo que el plazo entre la convocatoria y la presentación de propuestas no podrá ser menor a veintidós (22) días hábiles.

- El Comité de Adquisiciones podrá continuar con el proceso de adquisición y contrataciones aún cuando exista una única oferta válida, siempre que cumpla con todos los requisitos exigidos en las bases.

- Los procesos de nivel II y III preverán un plazo mínimo de 3 días hábiles posteriores a la convocatoria, para que los participantes formulen consultas y observaciones y un plazo máximo de 3 días hábiles para que el Comité emita las respuestas aclaratorias y otras acciones que se consideren de utilidad para obtener ofertas que cumplan con las condiciones indicadas. Estas fechas estarán incluidas en las bases.

- Mediante las consultas, para el caso de los niveles II y III, los participantes podrán solicitar la aclaración de cualquiera de los extremos de las bases o plantear solicitudes respecto a ellas. Mediante escrito debidamente fundamentado, los participantes podrán formular observaciones, las que deberán versar sobre el incumplimiento de lo señalado en las bases.

- El Comité de Adquisiciones absolverá las consultas y observaciones mediante un mismo pliego absolutorio, debidamente fundamentado, el que deberá contener la identificación de cada participante que les formuló las consultas presentadas y las respuestas a cada una de ellas.

- El pliego de absolución de consultas y observaciones se integrará a las bases, constituyendo las bases integradas las reglas definitivas del proceso de contratación y serán publicadas en la página WEB del Banco, junto con el Acta de Integración.

- El pliego absolutorio de consultas y observaciones también se considerará como parte integrante de la orden de compra, orden de servicio o contrato, según corresponda.

b) Recepción de Propuestas

- La recepción de las propuestas debe efectuarse de acuerdo con los plazos, oportunidades y medios indicados en las Bases y/o documentos complementarios o aclaratorios en la mesa de partes del Banco o lugar que se indique en las Bases. Para que una propuesta sea admitida deberá incluir la documentación de presentación obligatoria que se establezca en las Bases.

- 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 o traductor colegiado certificado, 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.

- El plazo mínimo entre la absolución de consultas y la presentación de propuestas es de 3 días hábiles.

- Cuando se exija la presentación de documentos que sean emitidos por autoridad pública en el extranjero, el postor podrá presentar copia simple de los mismos sin perjuicio de su ulterior presentación, la cual necesariamente deberá ser previa a la firma del contrato. Dichos documentos deberán estar debidamente legalizados por el Consulado respectivo y por el Ministerio de Relaciones Exteriores, en caso sea favorecido con la Buena Pro.

- El proceso de recepción de las propuestas debe considerar los medios, oportunidad y resguardos necesarios para mantener las condiciones de transparencia y equidad.

- Las propuestas se presentarán en dos sobres cerrados, uno conteniendo la propuesta técnica y el otro la propuestas económica.

- En los procesos de selección correspondientes al II y III nivel, la recepción de propuestas y otorgamiento de la buena pro se efectuará en acto público, en el caso del I nivel de contratación dichos actos serán privados.

- Las propuestas presentadas deberán cumplir con todo lo requerido en las Bases, adjuntado los documento que se hubiesen solicitado.

- Las propuestas económicas deberán incluir 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, servicio u obra a adquirir o contratar; excepto la de aquellos postores que gocen de exoneraciones legales. El monto de la propuesta económica y los subtotales que componen serán expresados con dos decimales.

- Los integrantes de un consorcio no podrán presentar propuestas individuales ni conformar más de un consorcio en un proceso de selección, o en un determinado artículo cuando se trate de procesos de selección según relación de artículos.

- Los representantes de cada una de las empresas que firman la promesa de consorcio deberán contar con facultades suficientes para suscribir este tipo de contratos, debidamente inscritas en Registros Públicos. La verificación de los poderes se realizará al momento de la evaluación del expediente técnico y, de advertirse que alguno de dichos representantes carece de dichos poderes, se procederá a su descalificación.

- Cuando se trate de un acto público de presentación de propuestas, éste se realizará con la presencia de un notario público. Se empezará a llamar a los participantes en el orden en que se registraron para participar en el proceso, para que entreguen sus propuestas. El Comité de Adquisiciones procederá a abrir los sobres que contienen la propuesta técnica de cada postor y comprobará que los documentos presentados por cada postor sean los solicitados por las Bases. De no ser así, devolverá la propuesta, teniéndola por no presentada. Si las Bases han previsto que la evaluación y calificación de las propuestas técnicas se realice en fecha posterior, el notario 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, conservándolos hasta la fecha en que el Comité de Adquisiciones, en acto público, comunique verbalmente a los postores el resultado de la evaluación de las propuestas técnicas.

- Cuando se trate de un acto privado de presentación de propuestas, los participantes presentarán sus propuestas en sobre cerrado, en la dirección, en el día y el horario señalados en las Bases.

- Si existieran defectos de forma, tales como errores u omisiones subsanables en los documentos presentados que no modifiquen el alcance de la propuesta técnica, el Comité de Adquisiciones otorgará un plazo entre uno (1) o dos (2) días hábiles, desde el día siguiente de la notificación de los mismos, para que el postor los subsane, en cuyo caso la propuesta continuará vigente para todo efecto, a condición de la efectiva enmienda del defecto encontrado dentro del plazo previsto, salvo que el defecto pueda corregirse en el mismo acto.

- Constituyen documentos de presentación obligatoria:

a. Copia Simple de la Constancia de Inscripción vigente en el Registro Nacional de Proveedores.
b. Formatos solicitados en las Bases como documentación de presentación obligatoria.
c. De ser el caso, copia de la documentación de sustento para acreditar el cumplimiento de los términos de referencia o especificaciones técnicas, y cualquier otro documento que las Bases hayan considerado como tales.

- Constituyen documentos de presentación facultativa:

Documentación que sustente el cumplimiento de los factores de evaluación.

c) Evaluación de Propuestas

- El Comité de Adquisiciones incluirá en las bases los criterios que utilizará para evaluar las propuestas, el puntaje que asignara a cada uno de estos criterios y precisará qué documentación debe presentarse para obtener tal puntaje, en función del objeto de cada contratación. Dichos criterios deben ser objetivos y tener relación directa con el objeto de la convocatoria.

- El puntaje otorgado a los postores por la acreditación del cumplimiento de cada criterio de evaluación, será decisión del Comité de Adquisiciones, debiéndose incorporar en las bases el puntaje que se otorgará por el cumplimiento de cada factor de evaluación.

- La propuesta económica presentada deberá ser igual o menor al valor referencial, incluyendo todos los tributos, seguros, transportes, inspecciones, pruebas y, de ser el caso, los costos laborales, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien, servicio u obra a adquirir o contratar.

Evaluación:

- La calificación y evaluación de las propuestas es integral, realizándose en dos (2) etapas. La primera es la técnica, cuya finalidad es calificar y evaluar la propuesta técnica, y la segunda es la económica, cuyo objeto es calificar y evaluar el monto de la propuesta.

- Las propuestas técnica y económica se evalúan asignándoles puntajes de acuerdo a los factores y criterios que se establezcan en las Bases del proceso, así como a la documentación que se haya presentado para acreditarlos.

- En ningún caso y bajo responsabilidad del Comité de Adquisiciones que aprueba las Bases se establecerán factores cuyos puntajes se asignen utilizando criterios subjetivos.

- El procedimiento general de calificación y evaluación será el siguiente:

  - A efecto de la admisión de las propuestas técnicas, el Comité de Adquisiciones verificará que las ofertas cumplan con los requisitos de admisión de las propuestas establecidos en las Bases.

    - Sólo una vez admitidas las propuestas, el Comité de Adquisiciones aplicará los factores de evaluación previstos en las Bases y asignará los puntajes correspondientes, conforme a los criterios establecidos para cada factor y a la documentación de sustento presentada por el postor.

    - Las propuestas que en la evaluación técnica alcancen el puntaje mínimo fijado en las Bases, accederán a la evaluación económica. Las propuestas técnicas que no alcancen dicho puntaje serán descalificadas en esta etapa.

- Los miembros del Comité de Adquisiciones no tendrán acceso ni evaluarán a las propuestas económicas sino hasta que la evaluación técnica haya concluido.

- A efectos de la admisión de la propuesta económica, el Comité de Adquisiciones verificará que el monto ofertado no exceda el valor referencial, pudiendo el postor ofertar por debajo de este. Las propuestas que excedan del valor referencial serán descalificadas.

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

$$Pi = (Om \times PMPE)/Oi$$

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

- La evaluación de propuestas se sujeta a las siguientes reglas:

1. Etapa de evaluación técnica:

a) El Comité de Adquisiciones y Contrataciones evaluará cada propuesta de acuerdo con las Bases y conforme a una escala que sumará cien (100) puntos.
b) Para acceder a la evaluación de las propuestas económicas, las propuestas técnicas deberán alcanzar el puntaje mínimo de sesenta (60), salvo en el caso de la contratación de servicios y consultoría en que el puntaje mínimo será de ochenta (80).

Las propuestas técnicas que no alcancen dicho puntaje serán descalificadas en esta etapa.

2. Etapa de evaluación económica:

El puntaje de la propuesta económica se calculará siguiendo las pautas señaladas, donde el puntaje máximo para la propuesta económica será de cien (100) puntos.

3. Determinación del puntaje total:

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

- Tanto la evaluación técnica como la evaluación económica se califican sobre cien (100) puntos. El puntaje total de la propuesta

será el promedio ponderado de ambas evaluaciones, obtenido de la aplicación de la siguiente fórmula:

.

PTPi = c1PTi + c2PEi
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
c2 = Coeficiente de ponderación para la evaluación económica

- Los coeficientes de ponderación deberán cumplir las siguientes condiciones:

  a) La suma de ambos coeficientes deberá ser igual a la unidad (1.00).
  b) Los valores que se aplicarán en cada caso deberán estar comprendidos dentro de los márgenes siguientes:
     b.1) En todos los casos de contrataciones se aplicará las siguientes ponderaciones:
     $0.60 < c1 < 0.70$; y
     $0.30 < c2 < 0.40$

- La propuesta evaluada como la mejor será la que obtenga el mayor puntaje total.

d) Adjudicación:

- El Comité de adquisiciones otorgará la buena pro al postor que haya obtenido el mayor puntaje. En los procesos correspondientes al segundo y tercer nivel, la evaluación económica y el otorgamiento de la buena pro se realizarán en acto público y se entenderá notificada en el mismo acto. En el caso del primer nivel, la buena pro se otorgará en acto privado. En todos los casos, se notificará la Buena Pro a través de su publicación en la página web del Banco.

- La labor del comité de adquisiciones concluye con el consentimiento de la Buena Pro, entregando el expediente del proceso al Departamento de Logística.

- El Departamento de Logística comunicará al postor ganador la buena

- pro, solicitará la documentación pertinente para cada caso y gestionará el envío de la orden de compra u orden de servicio o la suscripción del contrato respectivo.

- La suscripción de la orden de compra, orden de servicio o del contrato corresponderá a los funcionarios del Banco con poderes para poder realizarlo según el monto de la contratación, de conformidad con los límites establecidos en el Régimen de Poderes del Banco para la contratación de bienes, servicios y obras. En el caso de la suscripción de un contrato, éste quedará formalizado cuando el Banco y el representante legal del postor suscriban el documento que lo contiene.

- En casos debidamente calificados podrá declararse desierto un proceso de adquisiciones o contrataciones. El comité de adquisiciones respectivo deberá establecer en el acta de desierto, las circunstancias que sustenten tal decisión, entre ellas se consideran las que como resultado de la evaluación no quede ninguna propuesta válida. La determinación de declarar desierto se publicará en la página web del Banco.

- Dentro de los dos (02) días hábiles siguientes al otorgamiento de la Buena Pro, los postores podrán interponer un recurso de apelación contra éste. El citado recurso deberá precisar los fundamentos de hecho y/o de derecho que lo sustenta; asimismo, deberá adjuntarse al mismo los medios probatorios respectivos y una carta fianza de garantía por la interposición del recurso, el que será por un monto equivalente al 5% del Valor Referencial del proceso de selección. La garantía no puede ser menor a una (1) UIT. El recurso deberá ser resuelto por el Gerente General en un plazo máximo de 5 días hábiles, debiendo la Resolución respectiva contar con un informe técnico y legal de sustento, así como encontrarse debidamente motivada. De declararse infundada o improcedente la apelación, se procederá a ejecutar la referida carta fianza.

- En caso no interponerse apelación dentro de los dos días hábiles de otorgada la Buena Pro, se procederá a emitir la orden de compra, de servicio o contrato, según corresponda. En aquellos supuestos, en los cuales solo se hubiese presentado un postor, se podrá emitir la orden de compra, de servicio o suscribir el contrato, de manera inmediata, previa remisión de la documentación solicitada en las bases, de ser el caso.

- En caso de declararse desierto un proceso de selección perteneciente a los Niveles II y III, se convocará a un proceso de selección de Nivel I, manteniendo las mismas formalidades que se tuvieron para el proceso principal que fue declarado desierto, respecto al Comité y la presentación de propuestas.

e) De las Garantías

- Las garantías se otorgarán a través de cartas fianzas, las que deberán ser emitidas por empresas financieras autorizadas por la Superintendencia de Banca, Seguros y AFP (SBS), o bancos incluidos en la lista actualizada de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú. Las cartas fianzas deberán ser incondicionales, solidarias, irrevocables y de realización automática en el país, al sólo requerimiento de Agrobanco. Se establecen los siguientes tipos de garantía:

  - Garantía por Adelanto

    - El Banco sólo puede entregar los adelantos previstos en las Bases contra la presentación de una garantía emitida por idéntico monto y un plazo mínimo de vigencia de tres (3) meses, renovable periódicamente por el monto pendiente de amortizar, hasta la amortización total del adelanto otorgado. La presentación de esta garantía no puede ser exceptuada en ningún caso, en el cual se pida el adelanto.

- Cuando el plazo de ejecución contractual sea menor a tres (3) meses, las garantías podrán ser emitidas con una vigencia menor, siempre que cubra la fecha prevista para la amortización total del adelanto otorgado.

- Tratándose de los adelantos de materiales, la garantía se mantendrá vigente hasta la utilización de los materiales o insumos a satisfacción del Banco, pudiendo reducirse de manera proporcional de acuerdo con el desarrollo respectivo.

- Las Bases podrán establecer adelantos directos al contratista, los que en ningún caso excederán en conjunto del treinta por ciento (30%) del monto del contrato. La entrega de adelantos se hará en la oportunidad establecida en las Bases. La amortización de los adelantos se hará mediante descuentos proporcionales en cada uno de los pagos parciales que se efectúen al contratista por la ejecución de la o las prestaciones a su cargo.

- Garantía por Fiel Cumplimiento

  - Como requisito indispensable para suscribir el contrato, a partir de 60 UIT, el postor ganador debe entregar al Banco la garantía de fiel cumplimiento del mismo. Esta deberá ser emitida por una suma equivalente al diez por ciento (10%) del monto del contrato original y mantenerse vigente hasta la conformidad de la recepción de la prestación a cargo del proveedor o contratista, en el caso de bienes y servicios, o hasta el consentimiento de la liquidación final, en el caso de ejecución y consultoría de obras

- Garantía por el monto diferencial de la propuesta

- Como requisito indispensable para suscribir el contrato, a partir de 30 UIT, cuando, en la contratación de servicios, la propuesta económica fuese inferior al valor referencial en más del 10%, o, en el caso de la adquisición o suministro de bienes, fuese inferior en más del 20%, el postor ganador deberá presentar una garantía adicional por un monto equivalente al 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, en el caso de bienes y servicios. Esta garantía no se solicitará en el caso de la contratación de obras.

- Las garantías se ejecutarán a simple requerimiento del Banco en los siguientes supuestos

  - Cuando el contratista no la hubiere renovado antes de la fecha de su vencimiento. Contra esta ejecución, el contratista no tiene derecho a interponer reclamo alguno.

  - Una vez culminado el contrato, y siempre que no existan deudas a cargo del contratista, el monto ejecutado le será devuelto a éste sin dar lugar al pago de intereses. Tratándose de las garantías por adelantos, no corresponde devolución alguna por entenderse amortizado el adelanto otorgado.

  - La garantía de fiel cumplimiento y la garantía adicional por el monto diferencial de propuesta se ejecutarán, en su totalidad, sólo cuando la

resolución por la cual la Entidad resuelve el contrato por causa imputable al contratista, haya quedado consentida o cuando por laudo arbitral consentido y ejecutoriado se declare procedente la decisión de resolver el contrato. El monto de las garantías corresponderá íntegramente a la Entidad, independientemente de la cuantificación del daño efectivamente irrogado.

- Igualmente, la garantía de fiel cumplimiento y, de ser necesario, la garantía por el monto diferencial de propuesta, se ejecutarán cuando transcurridos tres (3) días de haber sido requerido por la Entidad, el contratista no hubiera cumplido con pagar el saldo a su cargo establecido en el acta de conformidad de la recepción de la prestación a cargo del contratista, en el caso de bienes y servicios, o en la liquidación final del contrato debidamente consentida o ejecutoriada, en el caso de ejecución de obras. Esta ejecución será solicitada por un monto equivalente al citado saldo a cargo del contratista.

CAPÍTULO II

PERFECCIONAMIENTO DEL CONTRATO

a) Generación de Orden de Compra, Orden de Servicio o Contratos

- El resultado de la adjudicación se traduce en un documento formal que incluye las condiciones del acuerdo de adquisición o contratación.

- El referido documento contendrá, entre otros, según sea pertinente, los siguientes puntos: identificación de las partes contratantes, objeto de la compra o breve descripción del servicio, precio, plazo de entrega, el cual puede ser una orden de compra, orden de servicio o un contrato. El contrato debe formalizarse mediante la suscripción del documento que lo contiene, salvo en el caso de las contrataciones cuyo monto correspondan al nivel I, en los que el contrato podrá formalizarse con la recepción de la respectiva orden de compra u orden de servicio por parte del proveedor.

- Para el caso de contratos, se utilizará el modelo de contrato estandarizado, tanto para bienes como servicios, establecido con el Área Legal.

- En todos los Niveles de Selección, el plazo máximo para la emisión de la Orden o la suscripción del Contrato es de 10 días hábiles, luego de que la Buena Pro quede consentida.

- La firma de todo documento oficial dirigido a un postor, en cualquier etapa del proceso de adquisición o contratación e independientemente de nivel que deba aprobar la adjudicación, residirá en la Gerencia de Administración o el Departamento de Logística.

- El Departamento de Logística enviará al Área Legal el proyecto de contrato y los documentos enviados por el Contratista (Ficha RUC, Vigencia de Poder actualizada, Testimonios de Constitución y modificación, copia de la Carta Fianza, entre otros detallados en las Bases), a fin de que el Área Legal revise y otorgue su conformidad a los datos consignados en el contrato y los documentos enviados por el proveedor, en caso corresponda la emisión de contrato.

b) Adicionales y reducciones

- Excepcionalmente y previa sustentación por el Unidad usuaria solicitante de la contratación, el Banco podrá ordenar y pagar directamente la ejecución de prestaciones adicionales en caso de bienes, servicios y obras hasta por el 25% de su monto, siempre que sean indispensables para alcanzar la finalidad del contrato. Asimismo, podrá reducir bienes, servicios u obras hasta por el mismo porcentaje. La aprobación de adicionales se realizará previa aprobación del Comité de Adquisiciones que aprobó el proceso.

- En caso de adicionales o reducciones, las garantías se ampliarán o reducirán proporcionalmente.

c) Contrataciones Complementarias

Dentro de los tres (3) meses posteriores a la culminación de un contrato para la adquisición de bienes, contratación de servicio o ejecución de obras, el Banco podrá contratar complementariamente bienes y servicios con el mismo contratista, hasta por un máximo del treinta (30%) del monto del contrato original.
La contratación de complementarios, se realizará previa aprobación del Comité de Adquisiciones que aprobó el proceso.

d) Recepción y certificación de bienes y servicios

- Las principales actividades que deben contemplarse en la recepción y certificación de bienes y servicios que adquiera o contrate el Banco son las siguientes:

    - Se verificará que lo recibido sea de acuerdo a lo solicitado por la Unidad Usuaria.

    - En el caso de servicios, la Unidad usuaria validará la conformidad del servicio y en el caso de bienes, la validación será realizada conjuntamente por el encargado del almacén o quien haga sus veces con la Unidad usuaria; respetando lo establecido en el procedimiento de almacenamiento de bienes.

    - Toda consultoría realizada deberá contar con la conformidad por parte del usuario solicitante. Esta conformidad deberá incluir la evaluación del resultado de la consultoría y la aplicación de la misma.

    - Tratándose de adquisiciones de edificaciones o ejecución de obras, la Gerencia General definirá un Comité con personal especializado, para la verificación técnica y conformidad respectiva.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCESO DE SELECCIÓN

CAPÍTULO I

GENERALIDADES

1. OBJETO DE LA CONVOCATORIA

El presente proceso de selección tiene por objeto la **ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB**.

2. VALOR REFERENCIAL

El valor referencial asciende a S/ 31,208.58 (Treinta y un mil doscientos ocho y 58/100 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 febrero de 2017.

3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante documento de fecha 20 de febrero de 2017.

4. 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.

5. ALCANCES DEL REQUERIMIENTO

El bien a adquirir está definido en el Capítulo III de la presente sección.

6. PLAZO DE ENTREGA

El plazo de entrega es de 15 días calendario, contados a partir del día siguiente de la entrega de la orden de compra.

CAPÍTULO II

DEL PROCESO DE SELECCIÓN

1. CRONOGRAMA DEL PROCESO DE SELECCIÓN

- ***Convocatoria……: 20/02/2017***
- ***Registro de Participantes……..: Del 21/02/2017 al 22/02/2017***
- ***Presentación de Propuestas……..: 22/02/2017***
  En acto privado: De las 09:00 a las 18:00 en la Avenida República de Panamá 3680 - 4to Piso - San Isidro
- ***Calificación y Evaluación de Propuestas……..: 23/02/2017***
- ***Otorgamiento de la Buena Pro……..: 24/02/2017***
  En acto privado: De las 09:00 a las 18:00 en la Avenida República de Panamá 3680 - 4to Piso - San Isidro

2. REGISTRO DE PARTICIPANTES Y ENTREGA DE BASES

El registro de los participantes se realizará de **manera gratuita** en la Oficina Administrativa de AGROBANCO, ubicada en Av. República de Panamá 3680 Cuarto Piso, en las fechas señaladas en el cronograma, en el horario de 09:00 a 16:00 horas y deberá adjuntarse copia de su RNP (Bienes).

El participante llenará el Formato Nº 01 de las Bases, donde constará el número y objeto del proceso, datos de la empresa, nombre y firma del representante Legal o apoderado, así como el día y hora de dicha recepción.

3. ACTO DE PRESENTACIÓN DE PROPUESTAS

En caso que la presentación de propuesta se realice en ACTO PRIVADO, deberá consignarse lo siguiente:

Los participantes presentarán sus propuestas en sobre cerrado, en la dirección, en el día y horario señalados en las Bases conforme a lo indicado en la sección general de las presentes Bases.

Las propuestas se presentarán en dos sobres cerrados y estarán dirigidas al Comité de Adquisiciones de la **ADQUISICIÓN DE NIVEL N° I,** conforme al siguiente detalle:

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

Señores
AGROBANCO
Av. República de Panamá 3680 Cuarto Piso
Att.: Comité de Adquisiciones

ADJUDICACIÓN DE NIVEL I N° 003-2017
Objeto del proceso: "Adquisición de renovación de solución de seguridad de antivirus, anti spam y filtro web"

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

Nº DE FOLIOS DE C/ EJEMPLAR

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

Señores
AGROBANCO
Av. República de Panamá 3680 Cuarto Piso
Att.: Comité de Adquisiciones

ADJUDICACIÓN DE NIVEL I N° 003-2017
Objeto del proceso: "Adquisición de renovación de solución de seguridad de antivirus, anti spam y filtro web"

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

Nº DE FOLIOS DE C/ EJEMPLAR

4. CONTENIDO DE LAS PROPUESTAS

SOBRE Nº 1 - PROPUESTA TÉCNICA:
Se presentará en un (1) original.

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

Documentación de presentación obligatoria:

- Copia simple del certificado de inscripción vigente en el Registro Nacional de Proveedores de OSCE: **Registro de Bienes**

- 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.**

- Declaración jurada y/o documentación que acredite el cumplimiento de los Requerimientos Técnicos Mínimos contenidos en el Capítulo III de de la presente sección. **Anexo Nº 02.**

- Declaración jurada en la que se compromete a mantener la vigencia de la oferta hasta la emisión de la orden de compra.- **Anexo Nº 03.**
  En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante legal común del consorcio.

- 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.

  Los representantes de cada una de las empresas que firman la promesa de consorcio deberán contar con facultades suficientes para suscribir este tipo de contratos, debidamente inscritas en Registros Públicos. La verificación de los poderes se realizará al momento de la evaluación del expediente técnico y, de advertirse que alguno de dichos representantes carece de dichos poderes, se procederá a su descalificación.

  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.

- Declaración jurada de plazo de entrega. **Anexo Nº 05**
- Declaración jurada de garantía técnica. **Anexo Nº 08**
- Lista de personal propuesto para cada punto del numeral 3.4 *Requerimiento de Personal* de las especificaciones técnicas, además:
    - Instalación de los productos ofertados
        - Copias de los certificados de estudios y certificados emitidos por el fabricante para el personal asignado a la instalación de las licencias de seguridad para endpoint.
        - Copias de los certificados de estudios y certificados emitidos por el fabricante para el personal asignado a la instalación de las licencias de seguridad para filtro de mensajería.
        - Copias de los certificados de estudios y certificados emitidos por el fabricante para el personal asignado a la instalación de las licencias de seguridad para filtro de contenidos.
    - Mesa de ayuda y soporte post venta
        - Copias de certificación ITIL
        - Copia de certificación en una de las soluciones endpoint, filtro de mensajería o filtro web.
        - Copia de certificación emitida por la marca en una de las soluciones solicitadas.
        - Declaración jurada simple sobre personal en planilla.
        - Consulta RUC en la web de SUNAT respecto a la cantidad de trabajadores y/o prestadores de servicio.
    - Capacitación de los productos ofertados
        - Copia de certificación por el fabricante en soluciones de seguridad para endpoint.
        - Copia de certificación por el fabricante en soluciones de filtro de mensajería.
        - Copia de certificación por el fabricante en soluciones de filtro web.
- Relación indicando marca y nombre de las soluciones ofertadas.
- Hoja de datos (datasheet) de cada solución.
- Carta del fabricante con referencia al proceso indicando dicho partnership. La carta, además, debe indicar el nivel de partner que el fabricante le asigna.

Muy importante:
La omisión de alguno de los documentos enunciados acarreará la no admisión de la propuesta.

Documentación de presentación facultativa
Criterios de Evaluación

a) La documentación referida al factor: Experiencia del Postor, deberá estar precedida de una relación detallada según el modelo del **Anexo N° 06.**

SOBRE N° 2 - PROPUESTA ECONÓMICA

El Sobre N° 2 deberá contener la siguiente información obligatoria:

a) Oferta económica y el detalle de precios unitarios cuando este sistema haya sido establecido en las Bases. (**Anexo Nº 07**)

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.

5. REQUISITOS PARA LA EMISION DE LA ORDEN DE COMPRA

a) Copia de DNI del Representante Legal;
b) Copia de la vigencia del poder del representante legal de la empresa no mayor a sesenta días de antigüedad.
c) Copia de la constitución de la empresa y sus modificatorias debidamente actualizadas, o vigencia de persona jurídica emitida por los Registros Públicos, en la cual se acredite la existencia de la empresa, se incluya los datos de su constitución y estructura de poderes vigentes refrendada y emitida por la SUNARP.
d) Copia del RUC de la empresa;
e) Contrato de consorcio con firmas legalizadas de los consorciados, de ser el caso.
f) Código de Cuenta Interbancario (CCI), de corresponder.

6. PLAZO PARA LA EMISION DE LA ORDEN DE COMPRA

El postor ganador de la buena pro deberá presentar toda la documentación requerida para la emisión de la orden en el plazo de 2 días hábiles. La citada documentación deberá ser presentada en Av. República de Panamá 3680 Cuarto Piso - San Isidro.

7. PLAZO PARA EL PAGO

La Entidad se compromete a efectuar el pago al contratista culminado los trabajos, en un plazo máximo de 10 días hábiles de otorgada la conformidad de recepción de la prestación.

8. FORMA DE PAGO

Para efectos del pago de las contraprestaciones ejecutadas, EL CONTRATISTA deberá presentar la siguiente documentación:

1. Factura correspondiente.
2. Copia de la orden de compra.

9. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del presente proceso, AGROBANCO le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde

F = 0.40 para plazos menores o iguales a sesenta (60) días.
F = 0.25 para plazos mayores a sesenta (60) días.

Las penalidades pueden alcanzar un monto máximo equivalente al diez por ciento (10%) del monto del contrato u orden vigente, o de ser el caso, del ítem que debió ejecutarse.

CAPÍTULO III

ESPECIFICACIONES TÉCNICAS

Objeto: "ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB"

I. OBJETO

AGROBANCO, a través del área de Sistemas, requiere la "ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD", que permita contar con soluciones de antivirus corporativo, filtro de correos (antispam) y filtro de páginas web, de acuerdo a las especificaciones técnicas que se detallan en el presente documento.

II. REQUISITOS QUE DEBERA CUMPLIR EL POSTOR

- El proveedor deberá estar inscrito en el Registro Nacional de Proveedores del Organismo Supervisor de las contrataciones del Estado, cuando se trate de un proceso de selección.
- El proveedor no deberá estar inhabilitado para contratar con el estado peruano.
- El proveedor debe tener más de 03 años de experiencia en el Perú implementando soluciones de antivirus, filtro de contenidos y filtro de correos de la marca ofertada.
- El proveedor deberá brindar garantía y soporte de los bienes suministrados, por el plazo de 1 año.

III. CARACTERÍSTICAS TÉCNICAS DEL BIEN

El postor deberá realizar la Instalación, configuración y/o actualización de las siguientes soluciones de seguridad:

Solución de seguridad – 700 licencias por 12 meses:

- Setecientos (700) licencias de seguridad para Endpoint
- Setecientos (700) licencias de seguridad para Filtro de Mensajería
- Setecientos (700) licencias de seguridad para Filtro de Contenidos

3.1. Solución de seguridad – 700 licencias por 12 meses:

El postor deberá considerar una solución de seguridad para 700 licencias para la entidad.

Las características de cada módulo de seguridad son las siguientes:

a) Setecientos (700) licencias de seguridad para Endpoint

La solución antivirus debe proteger a los siguientes sistemas operativos, puestos de trabajo fijos y móviles (portátiles) en las plataformas Intel y AMD, los sistemas operativos: Windows 7, Windows vista, Windows 8, Windows 8.1 y posteriores.

La solución de antivirus para la protección de puestos de servicios debe contar con al menos las siguientes capacidades de protección:

Protección Web

- La solución de antivirus, deberá contar con un sistema basado en la reputación de sitios web del fabricante de la solución, que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.

- El sistema de manejo de la reputación de archivos deberá estar integrado en la misma consola de antimalware como parte de la misma solución.
- De manera independiente el sistema de reputación de sitios web podrá implementarse por separado y poder integrarse a la consola de antimalware.
- Manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro de la red corporativa.
- Manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran fuera de la red corporativa.
- Permitir reclasificar sitios web.
- El sistema de protección Web no deberá depender de ningún explorador en específico.
- Permitir editar la lista de URL para permitir acceso a URL´s que se encuentran bloqueadas (razón sitio de mala reputación o interna) a nivel general, grupos o personal.

Protección contra infecciones de malware

- Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
- Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
  - Procesos que se ejecutan en la memoria principal (RAM)
  - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
  - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
  - Archivos recibidos a través de software de comunicación instantánea (MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
  - Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
  - La detección heurística de virus desconocidos.

Métodos de escaneos

- Manejar un sistema basado en distribución de firmas de malware desde la consola principal hacia las estaciones de trabajo. (método convencional).
- Manejar un sistema adicional de consulta de firmas de malware basado en reputación de archivos. Utilizando tecnología de Cloud Computing.
- La consola de antimalware podrá administrar los dos métodos de disponibilidad de firmas a todas las estaciones de trabajo reportadas en la consola, por grupo o por estación de trabajo.
- La consola de antimalware permitirá ver el estado de la consola que administra las firmas basadas reputación de archivos.
- En la consola se podrá ver estatus de las estaciones de trabajo que se encuentran operando en un modo convencional o en modo basado en firmas en la nube y que se encuentran en línea o fuera de línea.
- El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera integrada y visualizada desde la misma consola de antimalware.
- El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera independiente (stand alone) y visualizada desde la misma consola de antimalware.
- Manejar actualizaciones incrementales tanto del servidor a la nube, como del servidor a los clientes sin que estás sobrepasen de 100K.

Control de dispositivos

- Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.
- La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.

- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario tenga un control total sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario únicamente tenga permisos de solo lectura sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario tenga únicamente permisos de lectura y ejecución sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá evitar que el usuario pueda tener acceso al contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.

Reporte de amenazas a los laboratorios.
- Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
- Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.

Utilización de CPU
- Selección del nivel de utilización de CPU mientras se realiza un escaneo Programado, manual o desde la consola.
- La solución de antimalware podrá manejar niveles de uso del CPU cuando el usuario ejecute un escaneo manual, dicha configuración deberá manejarse de manera centralizada por el administrador.
- La solución de antimalware podrá manejar niveles de uso del CPU cuando se programen los escaneos a las estaciones de trabajo, dicha configuración deberá manejarse de manera centralizada por el administrador.
- La solución de antimalware podrá manejar niveles de uso del CPU cuando el usuario ejecute desde la consola de antimalware, dicha configuración deberá manejarse de manera centralizada por el administrador.

Informe de cumplimiento
- Garantizar que los clientes tengan los servicios activos, últimos componentes, consistencia en configuraciones y que han corrido escaneos regularmente.

Administración
- La solución debe garantizar la seguridad a través de SSL para las comunicaciones entre el servidor y la dirección web de la consola.

Login
- Integración con Active directory para la asignación de roles y permisos de Acceso a las configuraciones de la consola.

Resumen de sistema
- Visualizar, de forma rápida y sencilla, el estado de las estaciones de trabajo y servidores en una sola pantalla de Summary.
- Visualizar, de forma rápida y sencilla, el estado y estadísticas de las infecciones generadas y permitir también visualizar las estaciones de trabajo y servidores donde ocurrió la detección o infección.

- Visualizar, de forma rápida y sencilla, un resumen del estatus de las actualizaciones de firmas en las estaciones de trabajo y servidores, cantidad de equipos actualizados y desactualizados.

Manejo de grupos
- Agregar, modificar o eliminar Grupos para administración de los clientes con políticas diferentes

Logs
- Petición de Log de amenazas, actualizaciones y estado del servidor.

Configuraciones
- Aplicar configuración de políticas por servidor o estación de trabajo, por grupo o por usuario de manera independiente.
- Manejo de configuraciones
- Importar o Exportar configuraciones de políticas de un grupo de estaciones de trabajo a otro.
- Habilitar o deshabilitar el firewall de acuerdo a la ubicación física de usuario así como personalización de las políticas o excepciones.
- Lanzar una política de seguridad en caso de epidemias.
- Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.
- Personalizar los permisos de los clientes para realizar acciones en el software local.
- Petición de Actualización de patrones, configuraciones y software de forma inmediata.
- Lanzamiento de escaneos manuales a unidades del sistema o archivos mediante la consola del cliente o la navegación del explorador de Windows.
- Visualización Inmediata de los logs generados en los diferentes componentes de la solución.
- Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.

Clientes fuera de la red
- Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

Integración con Active Directory
- Integración de la solución con un dominio de Active Directory.
- Permitir la integración con Active Directory aún si el equipo en donde se instalará una consola de administración antivirus no se encuentra en el dominio.
- Permitir generar un análisis, listado de equipos que cuenten o no con una protección antimalware, basado en dominios o grupos del Active Directory.
- Apoyar múltiples dominios de confianza y los bosques de Active Directory;
- Utilizar la clave de cifrado antivirus que se encuentren en conformidad con Active Directory para realizar una conexión segura entre el servidor y el controlador de dominio de antivirus;
- Permitir a los clientes del árbol de directorios del antivirus, sea un reflejo del árbol de directorios de Active Directory.

Administración centralizada
- La solución antivirus debe poseer una consola de administración centralizada a la cual debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia.

Instalación clientes
- Paquete de instalación. Integración de la solución con un dominio de Active Directory.
- Consola Web. Instalación de cliente antivirus mediante la URL de la Consola de la solución.
- Línea de comandos. Instalación de cliente antivirus mediante línea de comandos o script.
- Remoto. Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
- Active Directory. Lanzamiento de instalación vía integración con el dominio de Active Directory.
- Segmentos de red. Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.

- Desinstalado automático. Desinstalación automática de otras soluciones para la instalación del cliente antivirus.

Desinstalación de clientes
- Manual. Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
- Remoto. Desinstalación del cliente de forma remota desde la consola de administración.

Actualización del servidor
- Manual. Petición de Actualización de patrones del servidor de forma manual.
- Automática. Configuración de Actualizaciones automáticas, así como la fuente de actualización.

Actualizaciones de clientes
- Manual y automáticamente desde consola. Distribución de actualizaciones a los clientes de manera Automática y Manual.
- Cliente sin conectividad al servidor. Actualización de sistema de firmas para clientes sin conectividad al servidor.
- Active Update. Actualización de grupo de usuarios por Agentes de Actualización o repositorios.

Consolidación de consolas de administración antivirus (Administración central)
- La solución deberá contar con una herramienta que consolide la administración de todas las consolas antivirus que se instalen.
- La consola de administración central deberá poder desplegar el licenciamiento a las demás consolas antivirus.
- La consola de administración central deberá ser el repositorio de logs y actualizaciones de todas las consolas antivirus.
- La consola central de administración deberá permitir replicar configuración.
- La consola central de administración deberá permitir y programas reportes consolidados.
- La consola de administración centralizada debe tener la capacidad de ser consultada mediante navegador web desde cualquier estación de trabajo que cuente con MS Internet Explorer.
- La consola debe permitir la creación de diversos usuarios para su administración y con diferentes niveles de acceso.
- La consola de administración centralizada debe tener la capacidad de notificar los intentos de infección de virus de acuerdo a parámetros definidos por el administrador de la solución.
- La consola de administración centralizada debe poseer la capacidad de actualizar las políticas de seguridad desde el fabricante en caso de una epidemia mundial de virus informativos.
- La consola de administración deberá de permitir características de administración proactiva para brindar a los administradores información y recomendaciones de políticas antes de la generación de patrones de virus. Políticas contra epidemias de virus
- La consola deberá permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre la solución de seguridad.
- Debe ofrecer administración centralizada de las consolas de los productos de antivirus de las diferentes capas de protección.
- Distribución automática y/o programada de actualizaciones para los distintos productos de antivirus desde cada 5 minutos.
- Reportes centralizados de incidencias de virus en distintos productos y plataformas de la misma suite de antivirus, generando estadísticas y análisis.
- Despliegue de políticas preventivas /reactivas para código malicioso en casos de alerta.
- Detección de amenazas asociadas con virus y software malicioso.
- Servicios de limpieza de daños en tiempo real y libre de agente para eliminar remanentes de virus, troyanos, sypware y entradas en el registro del sistema.
- Notificación inmediata y centralizada sobre ataques masivos de virus y/o código malicioso.
- El producto deberá soportar Instalación Local desde un CD, Conexión a red, etc.

Control de aplicaciones

- Para la prestación del Servicio de protección contra código malicioso en puestos de servicio se debe considerar una solución que evite que aplicaciones no autorizadas o maliciosas se ejecuten en los puestos de servicio.

b) Setecientos (700) licencias de seguridad para el Filtro de Mensajería

Para la protección del filtro de mensajería se requiere una solución que cumpla las siguientes características mínimas:

- Deberá poder instalarse sobre ambientes físicos o equipos virtuales vmware ESXi.
- Deberá estar basada en un sistema operativo de 64 bits.
- Deberá poderse implementar en esquemas de Alta Disponibilidad, dónde un equipo sea el responsable de la centralización de bitácoras y configuración de todos los equipos que forman parte de la arquitectura en Alta Disponibilidad.
- Deberá contar con actualizaciones para sus patrones y motores de detección de spam (en imágenes y heurística), phising y código malicioso.
- Deberá basarse en la comparación de la calificación final del correo después de ser analizado contra un umbral que podrá ser configurado.
- Deberá detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del Fabricante, permitiendo la configuración de umbrales para esta detección y la acción a tomar.
- Deberá soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Deberá revisar tanto el correo entrante como el saliente.
- Debe ofrecer capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Debe ofrecer el análisis de archivos comprimidos en los formatos más populares con 7 capas de compresión.
- Debe detectar el verdadero formato de un archivo sin basarse en el nombre, extensión o tipo MIME del mismo y poder aplicar acciones personalizadas ante su detección.
- Debe contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos de Microsoft Office, Adobe PDF y archivos de texto.
- Debe poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP como en políticas cuando el correo ya ha sido recibido.
- Debe ser capaz de recibir tráfico con conexiones TLS y poder hacer conexiones con otros servidores de TLS.
- Deberá contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Debe contar con mecanismos que permitan identificar los destinatarios de correo adecuadamente de tal forma que se pueda prevenir ataques de directorio y cosecha de información de directorios (Directory Harvest Attack). Para esto, es necesario que la solución pueda integrarse con múltiples servicios de directorio como Active Directory y OpenLDAP de forma simultánea y en múltiples dominios.
- Deberá contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen el dominio destino (correos de rebote o Bounced Mails).
- Deberá hacer un bloqueo automático de IPs debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.

- Deberá ser capaz de poder configurarse de tal forma que pueda haber excepciones, tanto en hosts remitentes como en destinatarios para asignar políticas diferentes.
- Deberá permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
- Deberá permitir la creación de políticas a nivel global por grupos o por usuario.
- Deberá de realizar la actualización de firmas de spam y códigos maliciosos en periodos configurables.
- Deberá contar con un método de respaldo de configuración de la solución.
- Deberá permitir el manejo de múltiples dominios, al menos 50 diferentes, para la limpieza de correo de spam y código malicioso.
- Deberá contar con protección anti-relay para correo de entrada o de salida basada en dominios, cuentas de correo y direcciones IP.
- Deberá contar con un método de revisión de mensajes en cuarentena basada en consultas, por remitente, asunto, destinatario y que permita revisar archivos adjuntos y cuerpos de mensaje, en formato texto.
- Deberá contar con sistema de revisión de logs de entrada y salida de tráfico de correo que permita realizar búsqueda de palabras, para su consulta rápida.
- Deberá poder, a solicitud de la Institución, almacenar el correo rechazado de forma temporal en la nube, por al menos 24 horas antes de ser eliminado.
- Deberá contar con tecnología heurística que permita detectar las actividades propias de un código malicioso, a fin de identificarlos y eliminarlos, aun siendo códigos maliciosos desconocidos. Además deberá poder proporcionar recomendaciones sobre la acción a tomar ante diferentes tipos de malware.
- Capacidad para evitar la fuga de información confidencial basada en expresiones regulares y palabras clave.
- Capacidad para evitar la fuga de información a través de plantillas predefinidas.
- Capacidad de detección de amenazas avanzadas y ataques dirigidos, a través del análisis automatizado de archivos adjuntos de correo electrónico en un ambiente de sandbox, el cual debe estar implementado en la infraestructura de la institución, no se aceptan sandbox de nube.
- El servicio deberá contar con la programación de reportes basados en plantillas para ser generados en períodos configurables con tablas y gráficos, y poder ser visualizados desde la consola de administración de la solución.
- El fabricante de la solución deberá contar con centros especializados en la investigación de amenazas
- La solución para la protección de correo electrónico externo debe tener capacidad para evitar la fuga de información confidencial basada en la detección de palabras clave (keyword) y expresiones regulares por protocolo SMTP.
- La solución debe tener la capacidad de integrarse a una consola central de administración, desde la cual se puedan administrar otras soluciones como la solución para la protección de la navegación web, antivirus y se puedan aplicar políticas para evitar la fuga de información confidencial desde un punto central tanto en el Gateway como en el endpoint.

c) Setecientos (700) licencias de seguridad para el Filtro de Contenidos Web

La solución propuesta por para brindar el presente servicio, deberá contar con las siguientes características tecnológicas:

- Deberá poder instalarse sobre ambientes físicos o equipos virtuales vmware ESXi y hyper-v montado sobre servidores Windows 2008 R2 y Windows Server 2012.
- La base de datos de categorías de la solución debe estar en la nube y poder ser consultada en tiempo real, no depender de actualizaciones o descargas locales para mejorar el nivel de la categorización.
- La solución debe contar con un mínimo de 82 categorías para filtrado de URLs

- La solución debe permitir la creación de categorias personalizadas de URL's, indicando la URL del sitio, dominio, palabras claves o una frase que identifique la URL del sitio.
- La solución debe permitir tomar acciones para URL's que aún no se encuentren categorizadas.
- Filtrado de URLs no productivas para el negocio, uso apropiado y disponibilidad del ancho de banda
- Filtrado de URLs maliciosas para incrementar la seguridad
- Filtrado de scripts maliciosos, objetos y contenido web
- Debe tener la capacidad de escaneo de malware en protocolos HTTPS
- Debe tener la capacidad de filtrado por categoría en protocolos HTTPS
- Capacidad de brindar la protección en tráfico HTTP, HTTPS y FTP.
- Permitir el manejo de la herramienta vía Web (HTTP o HTTPS).
- Para el filtrado por categoría la solución debe contar con al menos las siguientes acciones, monitoreo, bloqueo, cuotas de tiempo, acceso a categorías restringidas cuando el usuario proporcione un password definido por el administrador y notificar al usuario para permitir que el usuario elija continuar con el acceso al sitio o desistir.
- La solución debe tener la capacidad de aplicar filtros basados en el contenido de los headers del protocolo HTTP, y aplicar filtros que permitan limitar el uso de cierto tipo de navegadores identificándolos por el user agent, limitar el tamaño de los archivos que son subidos a sitios en internet, evitar que se hagan consultas de ciertas palabras en buscadores, evitar que se hagan post a sitios web y permitir solo la visualización del sitio, etc.
- Aceleración de tráfico mediante el uso de caching
- Monitoreo y reporteo
- La solución debe soportar el manejo del header X-Forwarded-for.
- La solución debe contar con la funcionalidad de control de aplicaciones, la cual debe permitir o bloquear la aplicación indicada, debe controlar un mínimo de 800 aplicaciones.
- Infraestructura global de bloqueo de páginas maliciosas basada en la reputación de seguridad de la misma
- Permitir la creación de políticas de control de accesos por día, por horario laboral y días específicos.
- Poseer características que permitan la consulta o recepción de nuevos patrones de seguridad de las siguientes formas:
- A partir de la consola Web, por medio de un sitio del fabricante del producto en Internet:
  - Descarga de paquetes incrementales.
  - Descargas programadas.
  - Descargas bajo demanda solicitadas manualmente.
- Deberá tener la capacidad de analizar y contener amenazas que puedan ser parte de un ataque dirigido.
- Deberá tener la capacidad de bloquear descargas por tipo de extensión de archivo.
- Deberá contar con la funcionalidad de detección, eliminación y prevención de amenazas y códigos maliciosos en tiempo real.
- Deberá poseer la característica de detección de virus, spyware, grayware, phishing, worms, troyanos y demás códigos maliciosos.
- Deberá contar con la característica de detectar código malicioso a través de patrones y/o heurística.
- Qué posea la característica de detección de tráfico malicioso proveniente de una botnet o el intento de comunicación desde un cliente de la red a una botnet y pueda controlarlo.
- Poseer las características de identificación y eliminación de código malicioso como consecuencia del acceso a las páginas Web con contenido de applets de Java, ActiveX, etc.
- Facilitar el almacenamiento de eventos (logs) del acceso de los usuarios a través de HTTP y FTP, así como también de códigos maliciosos encontrados a fin de hacer una investigación en el registro sin necesidad de utilizar herramientas de terceros, y generar informes consolidados.
- Poseer características que hacen respaldos de la configuración actual y restaurar la configuración del producto.
- Tener la capacidad de manejar el aislamiento para los archivos con malware o no reparables en áreas de cuarentena.

- Interactuar con servidores LDAP como Windows Active Directory y/o con Open LDAP.
- Posibilidad de instalarse en los siguiente modos: Transparent Bridge, ICAP server, Forward Proxy, Transparent usando WCCP y Reverse Proxy.
- Tener la capacidad escanear contenido HTTP y FTP de clientes que suben o descargan contenido a un servidor Web, protegiéndolo de amenazas.
- Tener la capacidad de integrarse con otros dispositivos proxy como (bluecoat y squid) para complementar la seguridad de la Institución.
- Ofrecer Alta Disponibilidad en modo Transparente Bridge.
- Integración con dispositivos ICAP como complemento a la seguridad de la Institución.
- Poseer el método de bloqueo de las descargas por tipo de archivo.
- Filtrado de URLs maliciosas a través de políticas por grupos de usuarios, IPs o grupos en el Directorio Activo.
- Filtrado de scripts maliciosos, objetos y contenido Web.
- Aceleración de tráfico mediante el uso de caché, para reducir la carga en los servidores y el consumo de ancho de banda.
- Los servidores de esta solución, deberán contar con acceso a Internet, de tal forma que se puedan conectar a los sitios del fabricante para alimentar las bases de datos de reputación y para obtener información de ellas para la consulta de sitios maliciosos.
- Se deberá tener la capacidad de inspeccionar trafico HTTP a través de sentencias o comandos integrados en los encabezados del paquete, permitiendo o bloqueando su ejecución
- Capacidad de validar la vigencia, autenticidad de certificados de sitios HTTPS
- Capacidad para evitar la fuga de información confidencial basada en expresiones regulares y palabras clave.
- Capacidad para evitar la fuga de información a través de plantillas predefinidas.
- Capacidad de detección de amenazas avanzadas y ataques dirigidos, a través de la integración automatizada con un sanbox para análisis de archivos en un ambiente de simulación local que resida en la infraestructura del cliente.
- La solución debe contar con un motor de escaneo de malware que tenga la capacidad de detectar malware tradicional, pero también cuente con capacidades de heurística para detectar amenazas nuevas.
- La solución debe contar con la capacidad de detectar y evitar la fuga de información confidencial a través de web, basándose en la identificación de información confidencial por palabras claves, y expresiones regulares.
- Debe contar con plantillas para la detección de información confidencial como mínimo PCI/DSS, SB-1386, GLBA.
- La solución debe verificar la fuga de información confidencial por protocolo FTP.
- La solución debe tener la capacidad de integrarse a una consola central de administración, desde la cual se puedan administrar otras soluciones como la solución para la protección de correo externo, correo interno, antivirus y se puedan aplicar políticas para evitar la fuga de información confidencial desde un punto central tanto en el Gateway como en el endpoint.

3.2. Instalación y puesta en producción

El servicio de instalación y configuración de la solución ofertada estará a cargo del postor y será llevado a cabo dentro de la zona de Lima Metropolitana.

3.3. Mantenimiento y Soporte técnico 24x7

Referente a toda la solución, se debe incluir el Servicio de Soporte y 02 Mantenimientos Preventivos al año (semestral) y Mantenimiento Correctivo por 01 año bajo la modalidad 24x7x365 (Lunes a Domingo) y un tiempo de respuesta no mayor a 2 horas, iniciándose ambos a partir de la firma de contrato bajo las siguientes condiciones:

a) El tiempo de respuesta deberá no ser mayor a 2 horas y un tiempo de resolución máximo de 8 horas

b) Los servicios de mantenimiento correctivo de las soluciones deberán estar disponibles sin límite de horas por intervención, ni cantidad de intervenciones mensuales del personal del proveedor; dándose por atendido un problema cuando es solucionado en su totalidad.
c) El personal técnico del proveedor, para solucionar un problema o incidente reportado, deberá apersonarse a las instalaciones de AGROBANCO, salvo que previamente y por mutuo acuerdo entre el personal técnico de ambas partes, se convenga que dicho soporte sea telefónico.
d) El postor proveerá información del estado del problema reportado.
e) Para situaciones que se pueden calificar como críticas, el proveedor deberá generar un procedimiento alternativo para evitar el problema o una solución temporal de parche en espera de una solución definitiva.
f) No podrá modificarse el nivel, calidad, periodicidad, categoría o cualquier otra característica de estos servicios durante el período de garantía, sin consentimiento de AGROBANCO.
g) Mano de obra y repuestos para cualquier servicio de atención por hardware.
h) Mantenimiento preventivo cada seis (06) meses en las instalaciones de AGROBANCO, en horario a coordinar con personal de Sistemas de AGROBANCO.
i) El Postor deberá contar con un centro de atención de requerimientos de servicios, de reparación o asistencia técnica o mesa de ayuda, de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con los servicios estipulado en las bases durante todo el tiempo de la garantía este servicio debe estar disponible 24x7x365.

Mantenimiento correctivo cada vez que se presente una falla o mal funcionamiento propio de la solución

3.4. Requerimiento de Personal

El postor deberá de contar con el siguiente personal técnico calificado:

Instalación de los productos ofertados

- **Licencias de seguridad para Endpoint:** Cinco (05) ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

- **Licencias de seguridad para Filtro de Mensajería:** Cinco (05) ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

- **Licencias de seguridad para Filtro de Contenidos:** Cinco (05) ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

Mesa de ayuda y Soporte Post Venta

Un (01) ingeniero de las especialidades de Ingeniería Electrónica, Sistemas ó Telecomunicaciones o a fines, con Certificación ITIL y con certificación en una de las soluciones de endpoint, filtro de mensajería o filtro web.
- Mínimo Tres (03) personas especialistas con certificación emitida por la marca solución ofertada.
- Declaración jurada simple sobre los ingenieros y/o técnicos que se presenten como personal certificado por el fabricante ofertado, se encuentre en planilla de la empresa postora como trabajadores, no se aceptará personal que esté en modalidad de prestación de servicios, para

dicho efecto, además se deberá adjuntar la consulta RUC en la web de la SUANT respecto de la cantidad de trabajadores y/o prestadores de servicio.

Capacitación de los productos ofertados

El Postor deberá realizar una capacitación de los productos ofertados con un total de doce (12) horas. El detalle de los cursos es el siguiente:

- Curso de cuatro (04) horas para soluciones de seguridad de endpoint. El instructor deberá estar certificado por el fabricante en soluciones de seguridad para endpoint.
- Curso de cuatro (04) horas para soluciones de filtro de mensajería. El instructor deberá estar certificado por el fabricante en soluciones de filtro de mensajería.
- Curso de cuatro (04) horas para soluciones de filtro web. El instructor deberá estar certificado por el fabricante en soluciones de filtro web.

- El postor en su propuesta deberá indicar la marca y nombre de las soluciones ofertadas, asi mismo deberá adjuntar la hoja de datos (Datasheet) de cada solución presentada.

  El postor deberá ser partner de los productos ofertados. Deberá adjuntar carta del fabricante con referencia al proceso indicando dicho partnership. Se deberá indicar además en la carta el nivel de partner que el fabricante le asigna.

3.5. Garantía

La garantía del postor por las soluciones que componen la oferta deberá ser por un año. Esto cubre el soporte de software y el derecho a contar con la última versión de las soluciones ofertadas por los fabricantes durante la duración del contrato.

3.6. Condiciones Finales

- El postor en su propuesta deberá indicar la marca y versiones de las propuestas ofertadas, así mismo deberá adjuntar el documento técnico (datasheet) de cada propuesta presentada.

- El Postor deberá ser partner de los productos ofertados. Deberá adjuntar carta del fabricante con referencia al proceso indicando que son partners de los productos ofertados. Se deberá indicar el nivel de partner.

IV. LUGAR DE ENTREGA DEL BIEN

Los bienes deberán ser ingresados en el Almacén AGROBANCO, ubicado en Calle Manuel Gonzáles Olaechea N° 415 San Isidro, Lima.

V. PLAZO DE ENTREGA DEL BIEN

El plazo de entrega es de 15 días calendario, contado a partir del día siguiente de la entrega de la orden de compra o suscripción del contrato.

VI. CONFORMIDAD DEL BIEN

Para efecto del trámite de pago, el Área de Sistema, deberá otorgar la conformidad del bien dentro de un plazo de 10 días hábiles de recibido los bienes.

CAPÍTULO IV

CRITERIOS DE EVALUACIÓN

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

Previamente a proceder a evaluar la documentación de carácter técnico, en el supuesto de haberse presentado una promesa formal de consorcio, deberá verificarse que los representantes de las empresas participantes posean las facultades suficientes para suscribir dicho tipo de contratos. Si se advirtiera que alguno de los representantes de dichas empresas careciera de estas facultades, se deberá descalificar al postor.

1. EXPERIENCIA DEL POSTOR: (80.00 puntos)

Se calificará considerando el monto facturado acumulado por el postor durante un periodo no mayor a ocho (8) años a la fecha de la presentación de propuestas, hasta por un monto máximo acumulado de cuatro (4) veces el valor referencial.

Tal experiencia se acreditará mediante contratos y la respectiva conformidad por la prestación efectuada 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). Los comprobantes de pago y/o contratos que se presenten deberán acreditar experiencia en SOLUCIONES DE SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN (ANTIVIRUS, FILTRO DE MENSAJERÍA, FILTRO DE CONTENIDOS WEB) CIÓN, CLASIFICACIÓN DE LA INFORMACIÓN o similares **(ANEXO 06).**

La asignación de puntaje será de acuerdo al siguiente criterio:

FACTORES REFERIDOS AL POSTOR	Puntos
CRITERIO	
• Monto acumulado igual o mayor a 4 veces el valor referencial	80.00
• Monto acumulado igual o mayor a 3 veces el valor referencial y menor a 4 veces el valor referencial.	70.00
• Monto acumulado igual o mayor a 1 vez el valor referencial y menor a 3 veces el valor referencial	60.00
• Monto menor a 1 vez el valor referencial	0.00

2) <u>CERTIFICADOS O CONSTANCIAS DE CUMPLIMIENTO DE PRESTACIÓN</u>: (20.00 puntos)

Se evaluará en función al número de certificados o constancias que acrediten que la prestación se efectuó sin incurrir en penalidades. Tales documentos deben referirse a todos los contratos que se presentaron para acreditar la experiencia del postor.

$$PCP = \frac{PF \times CBC}{NC}$$

Donde:

PCP = Puntaje a otorgarse al postor
PF = Puntaje máximo del Factor
NC = Número de contrataciones presentadas para acreditar la experiencia del postor
CBC = Número de constancias de buen cumplimento de la prestación

Asimismo, el factor podrá ser acreditado mediante la presentación de cualquier documento en el que conste o se evidencie que la prestación presentada para acreditar la experiencia fue ejecutada sin penalidades, independientemente de la denominación que tal documento reciba.

El postor deberá presentar copia simple de certificado(s) o constancia(s) de cumplimiento de prestación, el mismo que debe acreditar que la prestación se efectuó sin que haya incurrido en penalidades, no pudiendo ser mayor de veinte (20) contrataciones. El certificado o constancia deben referirse a los contratos que se presentaron para acreditar la experiencia del postor.

PARA ACCEDER A LA ETAPA DE EVALUACIÓN ECONÓMICA, EL POSTOR DEBERÁ OBTENER UN PUNTAJE TÉCNICO MÍNIMO DE SESENTA (60.000) PUNTOS.

Se aceptarán propuestas de los postores que cumplan con los requisitos ya exigidos y se calificará de acuerdo a los criterios de evaluación ya definidos

Para el otorgamiento de la Buena se utilizará la siguiente ponderación:

Propuesta Técnica : 0.6
Propuesta Económica : 0.4

FORMATO N° 01

REGISTRO DEL PARTICIPANTE

NIVEL DE CONTRATACION AL QUE SE PRESENTA:

Nivel I	(X)
Nivel II	( )
Nivel III	( )

Denominación del proceso: **ADQUISICION DE NIVEL I Nº 003-2017-AGROBANCO**

DATOS DEL PARTICIPANTE:

(1) Nombre o Razón Social:		
(2) Domicilio Legal:		
(3) R. U. C Nº	(4) Nº Teléfono (s)	(5) Nº Fax
(6) Correo(s) Electrónico(s):		

El que suscribe, Sr.(a): _____, identificado con DNI Nº_____, representante Legal de la empresa _____, que para efecto del presente proceso de selección, solicito ser notificado al correo electrónico consignado en el cuadro precedente, comprometiéndome a mantenerlo activo durante el período que dure dicho proceso.

Lima, _____de _____ de 2016

.....
Firma, Nombres y Apellidos del postor

ANEXO N° 01

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS
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	

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 DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

Presente.-

De nuestra consideración:

El que suscribe, ... (postor y/o Representante Legal de .....), identificado con DNI Nº ....., RUC Nº ..... en calidad de postor, luego de haber examinado los documentos del proceso de la referencia proporcionados por la Entidad .....**(Indicar nombre de la Entidad convocante)**, y conocer todas las condiciones existentes, el suscrito ofrece entregar ..... **(Describir el objeto de la convocatoria)**, 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, puede requerirse la presentación de otros documentos para acreditar el cumplimiento de los Requerimientos Técnicos Mínimos, conforme a lo señalado en el contenido del sobre técnico.

ANEXO N° 03

DECLARACIÓN JURADA

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

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 de la **ADJUDICACIÓN NIVEL I Nº 003-2017**, para la **ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB,** declaro bajo juramento:

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

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

3.- 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.

Ciudad y fecha, ...

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

ANEXO N° 04

PROMESA FORMAL DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

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 **ADQUISICIÓN NIVEL I Nº 003-2017**, 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.

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	Nombre, firma, sello y DNI del
Representante Legal empresa 1	Representante Legal empresa 2

ANEXO Nº 05

DECLARACIÓN JURADA SOBRE PLAZO DE ENTREGA

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

Presente.-

De nuestra consideración,

El que suscribe, don _____ identificado con D.N.I. N° _____, Representante Legal de _____, con RUC Nº _____, DECLARO BAJO JURAMENTO que mi representada se compromete a ejecutar el objeto del presente proceso en el plazo de _____ días calendario **(Indicar el plazo ofertado en días).**

Ciudad y fecha, ...

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

ANEXO N° 06

EXPERIENCIA DEL POSTOR

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

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 07

CARTA DE PROPUESTA ECONÓMICA

(MODELO)

Señores

COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

Presente.-

De nuestra consideración,

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

N°	CONCEPTO	PRECIO TOTAL S/.
1	**ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB**	

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 Nº 08

DECLARACIÓN JURADA DE GARANTÍA TÉCNICA

Señores
COMITÉ DE ADQUISICIONES NIVEL I - TEMAS TECNOLÓGICOS

Presente.-

De nuestra consideración,

El que suscribe, don _____ identificado con D.N.I. N° _____, Representante Legal de _____, con RUC Nº _____, DECLARO BAJO JURAMENTO que mi representada se compromete a ofrecer la garantía técnica de los bienes suministrados, por el plazo de 2 años a partir de la puesta en operación de los bienes (activación del servicio).

Ciudad y fecha, ...

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