BASES

ADQUISICION NIVEL I Nº 010-2021-AGROBANCO

"SUSCRIPCIÓN PARA LA SOLUCIÓN DE SEGURIDAD, ANTIVIRUS, ANTI SPAM Y FILTRO WEB"

2021

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.
- Ley N° 30893, Ley que modifica diversos artículos de la Ley Nº 29064, a efectos de fortalecer el Banco Agropecuario - AGROBANCO y establece facilidades para el pago de las deudas de sus prestatarios.
- 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.[1]
- 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.

[1] Ref: Título II: Portal de Transparencia, Art 5º del Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, aprobada por D.S. Nº 043-2003-PCM

- 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 aun 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 propuesta 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 x 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.2

- 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

[2] La Buena Pro se publicará el mismo día efectuado el acto.

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, siendo formalizadas a través de un acta.

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 contratación del **Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web.**

2. VALOR REFERENCIAL

El valor referencial asciende a S/ 127,146.73 (Ciento Veintisiete Mil Ciento Cuarenta y Seis con 73/100 Soles), incluido los impuestos de Ley y cualquier otro concepto que incida en el costo total del servicio. El valor referencial ha sido calculado al mes de setiembre de 2021.

3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante documento de fecha 20 de setiembre de 2021.

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 servicio a contratar está definido en el Capítulo III de la presente sección.

6. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio es de 365 días calendario, contados a partir del día siguiente de la entrega de la orden de servicio.

CAPÍTULO II

DEL PROCESO DE SELECCIÓN

1. CRONOGRAMA DEL PROCESO DE SELECCIÓN

- ***Convocatoria……..……: 20/09/2021***
- ***Registro de Participantes……..……: Del 21/09/2021 al 23/09/2021***
- ***Presentación de Propuestas……..……: 23/09/2021***
  En acto privado: De las 09:00 a las 18:00 en la Avenida República de Panamá 3531- Piso 9 - San Isidro
- ***Calificación y Evaluación de Propuesta Técnica……: Del 24/09/2021 al 27/09/2021***
- ***Evaluación Económica y Otorgamiento de la Buena Pro……..…: 28/09/2021***
  En acto privado: De las 09:00 a las 18:00 en la Avenida República de Panamá 3531- Piso 9 - San Isidro

2. REGISTRO DE PARTICIPANTES

El registro de los participantes se realizará **gratuitamente** de manera electrónica al correo gcelis@agrobanco.com.pe, en el horario de 09:00 a 18:00 horas. El participante deberá presentar el **Formato N° 01** de las Bases, donde constará el número y objeto del proceso, datos de la empresa, nombre y firma del representante legal o apoderado y deberá adjuntarse copia de su Registro Nacional de Proveedores – RNP (Servicios). La fecha y hora de recepción será registrada en el correo.

No se dará por recepcionado ningún registro fuera de la fecha y horario establecido en las Bases.

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 I N° 010-2021 "Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web",** conforme al siguiente detalle:

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

Señores
AGROBANCO
Av. República de Panamá 3531- Piso 9 - San Isidro
Att.: Comité de Adquisiciones Nivel I

ADJUDICACIÓN DE NIVEL I N° 010-2021
Objeto del proceso: "Suscripción para la Solución de Seguridad, Antivirus, Antispam 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 3531- Piso 9 - San Isidro
Att.: Comité de Adquisiciones Nivel I

ADJUDICACIÓN DE NIVEL I N° 010-2021
Objeto del proceso: "Suscripción para la Solución de Seguridad, Antivirus, Antispam 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 Servicios**
- 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 la presente sección - **Anexo Nº 02.**
- Declaración jurada en la que se compromete a mantener la vigencia de la oferta hasta la suscripción del Contrato - **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 sobre plazo de ejecución - **Anexo Nº 05.**

- Declaración jurada indicando contar con más de 01 año de experiencia en el Perú, implementando soluciones de antivirus, filtro de contenidos y filtros de correos de la marca ofertada, suscrita por el representante legal de la empresa.

- Declaración jurada donde se indique la marca y versiones de las soluciones ofertadas, así mismo deberá adjuntar el documento técnico (datasheet) de cada propuesta.

- Relación del personal propuesto para la instalación de los productos ofertados, y del personal de mesa de ayuda y soporte post venta. Se deberán adjuntar los siguientes documentos:

  - Copia de currículum vitae del personal que realizará la instalación de los productos ofertados (mínimo 2 personas); el cual deberá incluir los certificados emitidos por el fabricante de la marca presentada.

  - Copia de Currículum vitae del personal que atenderá Soporte Post Venta y mesa de Ayuda, adjuntado copia de título profesional de un (01) Ingeniero, con certificación en una de las soluciones de endpoint, filtro de mensajería o filtro web.

  - Copia de Currículum vitae del personal que atenderá Soporte Post Venta y mesa de Ayuda (mínimo 2 personas), adjuntando certificados emitidos por el fabricante de la marca presentada.

- Declaración jurada simple en la que se indique que el personal certificado por el fabricante se encuentra en planilla de la empresa postora como trabajadores. Además, se deberá adjuntar la consulta RUC en la web de la SUNAT respecto de la cantidad de trabajadores y/o prestadores de servicio.

- Carta del fabricante con referencia al proceso y/o entidad contratante indicando que son partners de los productos ofertados además deberá indicar el nivel de partner o canal.

- Declaración Jurada de Garantía - **Anexo Nº 06.**

- Declaración Jurada de Soporte - **Anexo Nº 07.**

Muy importante:

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

Documentación de presentación facultativa

Consignar la documentación que deberán presentar los postores para la aplicación de los factores de evaluación.

- Experiencia del postor - **Anexo Nº 08.**
- Declaración Jurada de capacitación ofrecida - **Anexo N° 09.**

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 10.**

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

5. DETERMINACION 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 = ***0.60***
c2 = Coeficiente de ponderación para la evaluación económica = ***0.40***

6. REQUISITOS PARA LA EMISIÓN DE LA ORDEN DE SERVICIO

Previo a la emisión de la orden de servicio, el postor ganador deberá presentar la siguiente documentación:

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) Declaración Jurada para proveedores y contrapartes, de acuerdo a formato enviado por la Entidad.
f) Código de Cuenta Interbancario (CCI), de corresponder.

7. PLAZO PARA LA EMISIÓN DE LA ORDEN DE SERVICIO

El postor ganador de la buena pro deberá presentar toda la documentación requerida para la emisión de la orden de servicio en el plazo de 2 días hábiles. Una vez notificado el proveedor, deberá entregar la citada documentación vía correo electrónico a gcelis@agrobanco.com.pe.

8. PLAZO PARA EL PAGO

La Entidad se compromete a efectuar el pago al contratista en un plazo máximo de 10 días calendario, de otorgada la conformidad de recepción de la prestación. [3]

9. FORMA DE PAGO

Para hacer efectivo el pago, **EL CONTRATISTA** deberá presentar ante la Oficina de Contabilidad de AGROBANCO la siguiente documentación:

1. Factura correspondiente.
2. Licencia electrónica donde se indique el Nombre del Cliente, el código de suscripción, la duración, cantidad de licencias y fecha de vencimiento.
3. Copia de los certificados entregados al personal que recibió la capacitación.
4. Acta de la capacitación realizada, firmada por el personal que recibió la capacitación y con el visto bueno de la División de Procesos y Tecnología de Agrobanco.
5. Copia de la orden de servicio.

10. 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:

Penalidad Diaria =	0.10 x Monto
	F x 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.

[3] Se aplica supletoriamente el Art. 171 del Reglamento de la Ley de Contrataciones del Estado.

CAPÍTULO III

TÉRMINOS DE REFERENCIA

Objeto: "SUSCRIPCION PARA LA SOLUCION DE SEGURIDAD, ANTIVIRUS, ANTISPAM Y FILTRO WEB"

I. OBJETO

AGROBANCO, a través de la División de Procesos y Tecnología, requiere la contratación del servicio de una solución de seguridad que incluya herramientas de antivirus corporativo, filtro de correos (antispam) y filtro de páginas web, de acuerdo con 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 01 año 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. DESCRIPCIÓN DEL SERVICIO

El postor deberá realizar la instalación, configuración y/o actualización de las siguientes soluciones de seguridad, pudiendo ser de diferentes fabricantes por un periodo de 12 meses:

- Quinientos noventa y uno licencias (551 Endpoint + 40 Servidores).
- Quinientos cincuenta y uno (551) licencias de seguridad para Filtro de Mensajería de Correo Electrónico.
- Quinientos cincuenta y uno (551) licencias de seguridad para Filtro de Contenidos HTTP.

Solución de seguridad para Endpoint (551 licencias):

Protección para Estaciones de Trabajo:
La solución para estaciones de trabajo debe brindar soporte a los sistemas operativos:
Windows 7, Windows 8 y Windows 10 32 y 64 bits.
MAC OS x 10.4.11 o superior.
Red Hat Enterprise Linux, CentOS, Ubuntu Server, Debian GNU/Linux, SUSE Linux Enterprise Server y Oracle Linux.
Debe brindar tecnología de protección capaz de eliminar amenazas de malware tales como virus, troyanos, spyware, adware, rookits u otro tipo de software malicioso que comprometa los sistemas de información.
Debe contar con un módulo de Exploit Prevention que impida que el malware explote vulnerabilidades de los sistemas operativos o aplicaciones que se ejecutan en la red.
Debe monitorear las aplicaciones mediante detección de comportamiento (Behavior Detection) para proporcionar una capa adicional de vigilancia y protección contra amenazas desconocidas.
Debe brindar la capacidad de análisis de reputación de archivos en la nube.
Debe brindar protección avanzada contra amenazas utilizando un enfoque de aprendizaje automático predictivo conocido como Machine Learning.
Debe permitir escanear archivos comprimidos.
Debe permitir remediación mediante el rollback de las acciones realizadas en el equipo por un software malicioso.
Debe contar con una tecnología que permita mejorar el performance de los escaneos en tiempo real, manuales o programados no realizando escaneos sobre archivos anteriormente revisados o que no hayan sido modificados.

Debe permitir el cambio de configuración a modo "en la nube" para los componentes de protección ofreciendo un nivel de seguridad óptima con un impacto mínimo en los recursos de los equipos y uso de ancho de banda de Internet.

Protección de correo electrónico:
Debe poder integrarse con Microsoft Outlook o Lotus.
Debe poder escanear a través de los puertos SMTP, POP3, IMAP, NNTP y MAPI.
Debe permitirnos seleccionar si se deseas escanear solo los correos entrantes o los correos entrantes y salientes.
Debe tener la opción de no escanear archivos comprimidos adjuntos.
Debe tener una opción de filtrado de archivos adjuntos, permitiendo especificar qué tipo de archivos serán renombrado o eliminados.

Protección web:
Debe poder analizar la data transferida mediante los protocolos HTTP, HTTPS y FTP.
Debe de permitir cambiar la acción que el antivirus realizará al detectar algún archivo infectado.
Debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus.
Debe tener la capacidad de proteger al usuario de ataques tipo phishing.
El antivirus debe tener una base de datos de enlaces URL que tienen contenido malicioso y que deben ser bloqueados automáticamente.

Protección de red:
El producto debe incluir un componente de Firewall y Host Intrusion Prevention:
El producto debe permitir crear reglas para restringir el tráfico de la red a través de puertos o protocolos específicos.
El producto debe permitir la creación de reglas que restrinjan la actividad de las aplicaciones.
Regula el acceso de las aplicaciones a datos confidenciales usando reputación local y en la nube sin afectar su rendimiento.
El producto debe ser capaz de reconocer las redes (zonas) en la cual se encuentra un equipo en la red.
Debe ser capaz de detectar ataques de red y bloquear al origen, impidiendo cualquier tipo de comunicación.
Debe de tener la capacidad de generar una lista de equipos confiables o direcciones IP a los cuales el componente de protección de red módulo no bloqueará.

La solución para estaciones de trabajo debe brindar las siguientes funciones de Control:

Control de aplicaciones:
El producto debe de permitir crear reglas que autoricen o bloqueen la ejecución de aplicaciones.
Debe de tener diferentes criterios para especificar las aplicaciones a bloquear, como la ruta de la carpeta que contiene el archivo ejecutable, Metadatos, Hash MD5, etc.
El producto debe de tener una lista de categorías de aplicaciones provista por el fabricante que permita una selección más organizada.
Debe permitir tener reglas activas, inactivas o en un estado de supervisión, en donde solo audite el acceso a las aplicaciones especificadas.

Control de navegación web:
El producto debe controlar el acceso a sitios web en los protocolos HTTP y HTTPS.
El componente de control web debe incluir clasificación de URLs en base a categorías que permita una selección más organizada, como por ejemplo Violencia, Chat, Redes Sociales, Pornografía, o cualquier otro contenido especificado en una lista de direcciones individuales.
Debe permitir especificar los usuarios o grupos a los que se les permite o bloquee el acceso a los recursos web descritos por una regla.
Debe permitir bloquear o advertir mediante notificaciones el acceso al sitio web que se considere potencialmente riesgoso o que no cumpla con las normas de productividad o buen uso del servicio.
Debe de tener integración con el Directorio Activo para especificar reglas por usuarios o grupos

Control de dispositivos:

Debe permitir bloquear por tipo de dispositivo de acuerdo con una lista predefinida que incluya como mínimo: USB, CD-ROM o medios de almacenamiento removibles.
Debe permitir añadir un nuevo tipo de dispositivo en función al ID de hardware o Cass ID.
Debe de tener integración con el Directorio Activo para especificar reglas por usuarios o grupos
Debe permitir manejar una lista de dispositivos de confianza.
Debe permitir especificar el acceso al dispositivo en modo de lectura o de lectura y escritura por usuarios.

Cifrado de Datos:
Debe permitir el cifrado de datos de manera centralizada para los siguientes medios de almacenamiento:
Discos duros: cifrado de archivos/carpetas o cifrado de disco completo
Dispositivos extraíbles: cifrado de archivos/carpetas o dispositivo completo.

Gestión de Sistemas:
El producto debe brindar funciones de gestión para Endpoint, esta función debe soportar los sistemas operativos Windows 7, Windows 8 y Windows 10 de 32 y 64 bits, estas características como mínimo deben ser las siguientes:
Debe escanear mediante la programación de una tarea todos los equipos de la red corporativa en busca de vulnerabilidades existentes en los sistemas operativos y aplicaciones para luego permitir distribuir los parches o actualizaciones necesarias con la finalidad de mantener la estabilidad y la seguridad de los Endpoint.
Debe sincronizarse con los servidores de Microsoft que brindan el servicio de Windows Update para descargar las actualizaciones y revisiones disponibles de los sistemas operativos y aplicaciones Microsoft para luego distribuirlas en la red.
Debe estar en capacidad de realizar tareas de inventario de software de los equipos de la red de modo que los administradores puedan controlar el uso de software.
Debe estar en capacidad realizar tareas el inventario de hardware en los Endpoint.
Debe brindar la capacidad por medio de la Consola de Administración de obtener informes personalizados de activos de hardware y licencias de software.

Protección para Servidores (40 licencias):

La versión para considerar deberá ser la versión top con la que cuentan para servidores.
El software antivirus debe poder instalarse en su última versión, sobre plataformas Windows Server 2003, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016 de 32 y 64 bits.
Red Hat Enterprise Linux, CentOS, Ubuntu Server, Debian GNU/Linux, SUSE Linux Enterprise Server y Oracle Linux, ya se la instalación en la nube del fabricante o localmente.
Debe brindar tecnología de protección como mínimo capaz de eliminar amenazas de malware tales como virus, troyanos, spyware, adware, rookits u otro tipo de software malicioso que comprometa los sistemas de información, lo que no quita presentar una solución que tenga mejores funcionalidades.
Debe brindar tecnología de protección capaz de eliminar amenazas de malware tales como virus, troyanos, spyware, adware, rookits u otro tipo de software malicioso que comprometa los sistemas de información.
Debe contar con un componente de protección contra malware, ransomware y anti-phishing en el tráfico originado por sesiones de usuarios en servidores con rol de Terminal Server, debe estar disponible para Microsoft Terminal Services y Citrix XenApp/Xen Desktop.
Debe brindar control de acceso web basado en categorías y aplicaciones a las sesiones de usuarios en servidores con rol de Terminal Server evitando riesgos de violación de datos, debe estar disponible para Microsoft Terminal Services y Citrix XenApp/Xen Desktop.
Debe contar con un módulo de Exploit Prevention que impida que el malware explote vulnerabilidades de los sistemas operativos o aplicaciones que se ejecutan en la red.
Debe monitorear las aplicaciones mediante detección de comportamiento (Behavior Detection) para proporcionar una capa adicional de vigilancia y protección contra amenazas desconocidas.
Debe detectar y bloquear ataques de ransomware en recursos compartidos mediante un sistema AntiCryptor el cual debe estar disponible para los sistemas operativos Windows Server, así como recolectar información sobre el usuario, equipo o dirección IP origen del ataque.

Debe brindar la capacidad de análisis de reputación de archivos en la nube.

Debe brindar protección proactiva utilizando un enfoque de aprendizaje automático predictivo conocido como Machine Learning.
Debe permitir escanear archivos comprimidos.
Debe permitir remediación mediante el rollback de las acciones realizadas en el equipo por un software malicioso.
Debe contar con un cache para el escaneo en tiempo real y escaneos programados, a fin de optimizar el consumo de recursos en servidores virtuales.
Debe contar con una tecnología que permita mejorar el performance de los escaneos en tiempo real, manuales o programados no realizando escaneos sobre archivos anteriormente revisados o que no hayan sido modificados.
Debe tener la capacidad de bloquear el tráfico entre las tarjetas de red de los servidores.
Debe contar con una función control de dispositivos que incluya como mínimo la capacidad de bloquear o permitir dispositivos de almacenamiento USB, CD/DVD-ROM, BLUETOOTH, etc.
Debe permitir manejar una lista de dispositivos de confianza.
Deberá contar con la capacidad de alertar en tiempo real cuando una modificación haya sido detectada en carpetas, archivos o llaves de registro del sistema operativo y aplicaciones, las alertas podrán ser enviadas por correo electrónico.
Debe permitir escanear el servidor y determinar qué aplicaciones está corriendo y operando actualmente en él.
Debe permitir ayudar a capturar amenazas que todavía no tienen Firma, incluyendo las amenazas de día cero.
Debe permitir especificar el acceso al dispositivo en modo lectura o de lectura y escritura.
Debe proteger sobre todas las vulnerabilidades conocidas y no conocidas en sistemas operativos Windows 2003 Server, Windows 2008 Server y superiores. Dicha protección debe prevenir la ejecución de ataques que intenten explotar dichas vulnerabilidades, independientemente de que el fabricante Microsoft ya no genere parches de seguridad para corregirlas.
Deberá contar con escaneos en tiempo real, escaneos programados y bajo demanda contra malware avanzado, virus y otros códigos maliciosos como son gusanos de red, spyware, troyanos, puertas traseras.
Deberá permitir que los escaneos en tiempo real, escaneos programados y bajo demanda deben contar con la posibilidad de manejar excepciones por al menos tipos de archivos y rutas.
Deberá contar con una funcionalidad que le permita elegir la acción a tomar de manera automática dependiendo del tipo de amenaza detectada.
Debe tener la capacidad reemplazar la solución antimalware y/o antivirus que actualmente use la institución.

Protección para equipos móviles.
El producto para dispositivos móviles debe poder instalarse sobre equipos con sistema operativos de Smartphone y Tablets basados en Android 4.1 o superior y iOS 9.0 o superior.
Debe brindar soporte MDM usando Microsoft Exchange ActiveSync.
Debe permite preconfigurar y desplegar aplicaciones de manera sencilla vía Google Play, App Store o su propio Self-Service Portal.
Debe brindar protección en tiempo real del sistema de archivos del dispositivo, interceptando y verificando todos los objetos trasmitidos usando conexiones Wireless, infrarrojo, Bluetooth, durante sincronismo con PC y al realizar descargas usando el navegador.
Verificación de los objetos en la memoria interna del dispositivo y en las tarjetas de expansión bajo demanda y de acuerdo con una programación.
Debe permitir filtro de llamadas y bloquear mensaje de texto non deseado.
Debe brindar funciones antirrobo como limpiar los datos personales, localizar el dispositivo, recibir el nuevo número en caso se reemplace el SIM Card.
Debe bloquear el acceso a las aplicaciones y los datos corporativos en dispositivos a los que se aplicado rooting o jailbreaking.
Permitir navegación segura en los navegadores compatibles con Android y iOS mediante el bloqueo de sitios phishing o maliciosos.
Aislar en un área de cuarentena los archivos infectados.
Configurar listas blancas y listas negras de aplicativos que se podrán ejecutar en el dispositivo.

Consola de administración centralizada.

La Consola de Administración debe permitir la configuración centralizada de cada una de las características y funciones de los productos de protección requeridos para estaciones de trabajo, servidores físicos o virtuales y dispositivos móviles.
El licenciamiento debe permitir desplegar la consola de administración íntegramente en Cloud, de manera On Premise, o en la nube pública de Microsoft Azure y AWS.
En el caso de ser On Premise debe instalarse sobre Sistemas Operativos Windows Server 2012 o superior y bases de datos SQL, Microsoft Azure SQL y MySQL, incluyendo entornos virtualizados.
La consola de administración deberá permitir la administración centralizada de equipos basados en Windows, Linux, Mac, Android y iOS.
El acceso a la Consola de Administración debe ser vía protocolo HTTPS.
El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros.
El producto debe ser capaz de mostrar los equipos detectados en la red.
El producto debe permitir al administrador visualizar características de la PC, tales como:

a) Sistema Operativo y versión.
b) Nombre de la PC y dirección IP.
c) Dominio al que pertenece.
d) Usuarios que han iniciado sesión el equipo.
e) Si es máquina virtual, tipo de máquina virtual.

La consola de administración debe de tener la capacidad de mostrar:

a) Software instalado en el equipo
b) Características de Hardware del equipo
c) Procesos que se están ejecutando

La consola de administración centralizada debe tener la capacidad de mostrar los archivos detectados por el antivirus en los equipos clientes.
La consola de administración debe ser capaz de poder tener múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus.
El producto debe tener la capacidad de crear políticas para usuarios móviles.
El producto debe ser capaz de detectar la red en la que se encuentra la PC y contactar de manera automática al servidor de políticas y actualizaciones correspondiente.
El producto debe ser capaz de controlar a través de políticas todos los componentes ofrecidos sin necesidad de usar otras consolas adicionales o productos de terceros.
La consola deberá permitir una estructura jerárquica para una mejor administración de los clientes antivirus.
Las políticas de administración de grupos deben poder heredar las políticas de grupos con mayor jerarquía.
Debe permitir la creación de políticas en modo de test para recopilar información sobre las aplicaciones que se ejecutan en la red y luego usarlas ajustar la configuración en producción.
La consola de administración debe permitir ver las actualizaciones de Windows Update que han sido instaladas y que faltan instalar en los equipos clientes.
El producto debe ser capaz de crear un paquete de instalación consolidado (archivo ejecutable) que puede ser accedido como recurso compartido o desde algún dispositivo extermino (CD, USB, etc.), para la instalación de los antivirus o del agente.
El producto deberá poseer un Log de eventos detallados.
Debe permitir la delegación de tareas mediante creación de usuarios basados en MS Active Directory con distintos perfiles de administración.
El producto debe ser capaz de escanear la red por Directorio Activo, Red IP o Dominios, en busca de nuevos equipos en la red.
El producto debe permitir la generación de reportes gráficos y personalización de los mismos y deben ser exportables a formatos XML, PDF y HTML
Los reportes deben ser personalizados y como mínimo deben ser:

a) Reportes de las maquinas más infectadas
b) Reportes de virus.
c) Reportes de Actualizaciones
d) Reportes de ataques de red

e) Reporte del estatus de la protección.

La consola debe ser capaz de permitir realizar un backups de sus configuraciones realizadas y de sus registros almacenados en su base de datos.
El producto debe ser capaz de generación de alertas ante un evento mediante el envío de un correo, o la ejecución de un archivo de lotes.
La comunicación debe ser cifrada entre servidores y clientes, usando certificados digitales provistos por el propio fabricante.
Las actualizaciones deben ser descargadas centralizadamente para que los clientes actualicen desde el servidor de administración sus definiciones de virus, phishing, actualización de parches del producto entre otras.
El producto debe ser capaz de actualizar las definiciones de virus de los paquetes de instalación a enviar, para de esta manera evitar el tráfico de red, que ocurre después de la instalación del producto.
El producto debe permitir crear categorías de aplicaciones, para autorizarlas o bloquearlas.
La consola deberá permitir visualizar todos los archivos que hayan sido desinfectados o eliminados en los equipos clientes, y tener la opción de restaurarlos si fuera necesario.
El servidor debe de permitir elegir cualquier equipo cliente como repositorio de actualizaciones y de paquetes de instalación, con el fin de optimizar el tráfico de red en sitios remotos, se debe poder especificar el ancho de banda.
La Consola debe contar con un indicador de nivel de protección de dispositivos móviles que permite evaluar el nivel de riesgo del dispositivo como alto, medio o bajo.
La consola de administración deberá contar con la capacidad de generación de roles personalizados.
Debe permitir auditar los cambios de configuración se aplicado por los administradores y compararla con otra revisión seleccionada.
La consola de administración deberá contar con un reporte dónde se indique las políticas sugeridas para la protección de vulnerabilidades en servidores y aplicaciones. Asimismo la solución deberá contar con la capacidad de integración con el Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio.

Endpoint Detection and Response

La solución debe permitir visibilidad en tiempo real, detección y respuesta automatizada de todas las actividades ejecutadas por 40 Endpoint.
La solución debe ser capaz de recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciber espionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.
La solución para estaciones de trabajo debe brindar soporte a los siguientes sistemas operativos: Windows 7, Windows 8 y Windows 10 32 y 64 bits.
Windows Server 2012, 2012 R2, Windows Server 2016 y Windows Server 2019 de 32 y 64 bits.
La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.
El agente EDR puede estar integrado o no a la solución de Endpoint Security, sin embargo debe ser del mismo fabricante.
La solución de EDR debe gestionar las políticas, agentes y reportes desde la misma Consola de administración del Endpoint Security.
El agente EDR se debe poder configurar por medio de una interfaz de línea de comandos.
La solución debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección, y luego tener la capacidad de aplicar una acción de respuesta.
La solución debe tener la capacidad de programar el escaneo en todos los puntos finales donde se ejecute el agente EDR con la información de IoC de acuerdo con una planificación del administrador.

La solución debe admitir la importación de IoC de terceros en formato Open IoC para su uso en el escaneo de los equipos.
La solución debe permitir tener visibilidad detallada del incidente relacionado con la amenaza detectada en un Endpoint, el incidente debe incluir como mínimo la siguiente información:

- Gráfico de la cadena de desarrollo de amenazas (Kill Chain).
- Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
- Información general sobre la detección, incluido el modo de detección.
- Cambios de registro asociados a la detección.
- Historial de presencia de archivos en el dispositivo.
- Acciones de respuesta realizadas por la aplicación.

La información de la cadena de desarrollo de la amenaza (Kill Chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre los procesos ejecutados en el dispositivo, conexiones de red, bibliotecas, llave de registro entre otras.
La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz como por ejemplo:

- Proceso de spawning
- Conexiones de red
- Cambios en el registro
- Descarga de archivos
- Dropped de objetos

El agente EDR debe tener un mecanismo de autodefensa para evitar que se modifique archivos relacionados con su funcionamiento como las entradas de componentes del sistema o un agente con similares características.

Solución de seguridad para el Filtro de Mensajería de Correo Electrónico: (551 licencias):
Deberá contar con un sistema de administración seguro vía Web (HTTPS).
Desde el sistema de administración centralizado se debe tener acceso a la creación de políticas entrantes y salientes, listas blancas y negras personales y globales, reportes, sistema de solicitud de soporte y cuarentenas.
La solución deberá poder configurarse como Gateway de correo electrónico para proteger el servicio de correo de la institución.
Para escalabilidad deberá permitir que su arquitectura de despliegue permita crear roles en diferentes servidores como por ejemplo centro de administración y motor MTA de escaneo.
La solución para el Gateway de correo deberá incluir el soporte para sistemas de archivamiento de correo y para la encriptación de mensajes.
Deberá integrarse con el protocolo LDAP y Directorio Activo para la autenticación de usuarios y creación de políticas.
Debe permitir ser implementado tanto en servidores (Appliance) físicos como en virtuales (virtual Appliance), deberá estar certificado para instalarse sobre VMware y Hyper-V.
Debe permitir la creación de más de 01 servidor de escaneo de AntiSpam y Antivirus para balancear la carga de mensajes y redundancia, cada servidor deberá tener las mismas políticas y deberá ser administrado desde una única consola centralizada.
Deberá incluir un filtro AntiSpam del mismo fabricante que soporte descargas automáticas de políticas Antispam. Deberá incluir varias técnicas de detección, como reputación de IP, heurística avanzada, huellas de mensajes y adjuntos, análisis de palabras clave, detección de direcciones web, etc.
El producto debe tener una efectividad de detección de SPAM fuera de caja de un mínimo del 98%. Deberá entregarse información del fabricante para certificar esta funcionalidad.
Deberá ofrecer una tecnología del mismo fabricante que permita el acceso en tiempo real a una amplia gama de información reciente contra spam. Este sistema es conocido como Sistema de Protección AntiSpam en tiempo real.
Deberá detectar ataques de robo de información (phishing), ataques de denegación de servicio (DoS) y cosecha de información (Harvest).
Deberá contar con un sistema de protección contra robo de información que permita filtrar los mensajes buscando palabras clave o patrones definidos tanto en el mensaje como en los adjuntos del correo.

Deberá contar con un sistema de filtro de contenido basado en "patrones" de búsqueda de contenido tanto en el mensaje como en los adjuntos del correo.
Deberá contar con un módulo específico para el Filtrado por Reputación que permite el bloqueo por IP's de servidores dudosos 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 10 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 Domain Keys.
Deberá de poder detectar, eliminar y limpiar virus y spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje y deberá ser del mismo fabricante.
Deberá de realizar el bloqueo de archivos adjuntos según el tipo o formato de archivo y no solo por la 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 contar con opciones para realizar pruebas de las políticas creadas antes que estas entren a producción y emitir reportes de fallos y correcciones que deben realizarse.
Deberá de poder hacer reglas de filtrado por dirección o dominio de correo electrónico.
Deberá de poder hacer creaciones de lista de aceptación y negación (blanca y negra) de dominios y usuarios (cuentas de correo) confiables.
Deberá de 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 y debe funcionar en un puerto distinto al del Administrador principal.

La consola debe permitir al administrador la visualización del contenido del repositorio de cuarentenas, analizar los correos retenidos por las políticas aplicadas y permitir tomar acciones como por eliminarlos o liberarlos.
Debe permitir el envío de correos electrónicos de compilación con el resumen del contenido de las casillas de correo individuales para cuarentena a todos los usuarios finales con un mensaje en cuarentena y al administrador del sistema. El envío debe ser automático, configurable en el periodo de envío y personalizable a criterio de la institución.
Mediante los correos de notificación los usuarios podrán consultar (previsualizar) los correos detenidos, para luego eliminar o liberar a su buzón los mensajes detenidos en la cuarentena, ya sea de manera selectiva o en su totalidad.
Tiempo de almacenamiento en cuarentena configurable. Debe permitir que los mensajes retenidos en cuarentena se eliminen automáticamente luego de un tiempo establecido por el administrador de acuerdo con las políticas de la institución.
Debe permitir a los usuarios finales el examinar su propia cuarentena mediante un acceso por URL, previa autenticación con su propia cuenta del dominio.
Independientemente del modelo de comercialización, la oferta deberá incluir el componente de generación y despliegue de informes y reportes.
El reporteador debe permitir visualizar y generar registros e informes multinivel y de auditoría gráficos y detallados para proporcionar visibilidad del tráfico SMTP en tiempo real (revisión o búsqueda de correos recibidos, enviados, filtrados, en cuarentena o rechazados por funcionalidades contra spam, entre otros). Los informes y reportes deberán ser configurables, personalizables y con diferentes niveles de detalle, a fin de obtener información tales como estadísticas tipo top ten (remitentes, tráfico de mensajes no deseados, destinatarios más atacados, malware detenido, entre otros) y registros de correos enviados y/o recibidos por un usuario específico, para usuarios individuales y grupos.
Debe permitir aumentar o disminuir los niveles de detalle, mediante funcionalidades tipo Drill Down o similares.
Debe permitir programar la generación de reportes automáticos en intervalos predeterminados (diario, semanal, mensual), a criterio de la institución.
Debe permitir la personalización y exportación de informes en formatos como PDF, HTML, CSV u otros.

Debe permitir obtener información relacionada al control de acceso discrecional (accesos a la consola administrativa), control de versiones y utilerías de restauración de configuración.

Solución de seguridad para el Filtro de Contenido HTTP (551 licencias):
La solución de filtro de contenidos web que inspecciona tráfico HTTP/HTTPS para proteger a los usuarios en la navegación contra malware o contenido inapropiado.
La solución propuesta por para brindar el presente servicio, deberá contar con las siguientes características tecnológicas:
Se podrá ofrecer como una solución On Premise o Cloud.
En el caso de ser On Premise deberá poder instalarse en modo de virtual appliance con hipervisores basados en VMware ESXi y Hyper-V
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 70 categorías para filtrado de URLs
La solución debe permitir la creación de categorías personalizadas de URL's, indicando la URL del sitio o dominio.
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 y HTTPS.
Permitir la gestión de la solución 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 y notificar al usuario para permitir que el usuario elija continuar con el acceso al sitio o desistir.
Bloqueo de páginas maliciosas basada en la reputación global de seguridad de esta 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 descarga de actualizaciones de nueva clasificación de categorías y seguridad por medio de un sitio del fabricante.
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 HTTPS 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.
Interactuar con servidores LDAP como Windows Active Directory.
Posibilidad de instalarse en los siguientes modos: Forward Proxy e ICAP Server.
Tener la capacidad escanear contra malware el contenido HTTP y HTTPS de clientes que suben o descargan a un servidor Web, protegiéndolo de amenazas.
Debe tener capacidad para configurar balanceo de carga y alta disponibilidad.
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.
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 tráfico 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 de detección de amenazas avanzadas y ataques dirigidos, a través de la integración automatizada con un Sandbox 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.

3.2. Instalación y puesta en producción

El servicio de 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 local por 01 año bajo la modalidad 24x7x365 (Lunes a Domingo) con 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 deberá ser mayor a 2 horas y un tiempo de resolución máximo de 8 horas que permitan la operatividad de AGROBANCO. Para temas complejos se deberá contemplar tiempos de resolución de 24 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 mediante acceso remoto, o 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 que permita la operatividad 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) 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:** Dos (02) especialistas como mínimo certificados en el producto ofertado. Adjuntar copia del certificado emitido por el fabricante.

- **Licencias de seguridad para Filtro de Mensajería:** Un (01) especialista como mínimo certificado en el producto ofertado. Adjuntar copia del certificado emitido por el fabricante.

- **Licencias de seguridad para Filtro de Contenidos:** Un (01) especialista como mínimo certificado en el producto ofertado. Adjuntar copia de certificados emitidos por el fabricante.

Mesa de ayuda y Soporte Post Venta
Un (01) ingeniero con certificación en una de las soluciones de endpoint, filtro de mensajería o filtro web.
- Mínimo dos (02) personas especialistas con certificación emitida por la marca solución ofertada.

Declaración jurada simple indicando que los especialistas solicitados que presenten como personal certificado por el fabricante, se encuentren 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 SUNAT respecto de la cantidad de trabajadores y/o prestadores de servicio.

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. ENTREGABLE

Deberá entregar una licencia donde se indique el Nombre del Cliente, el código de suscripción, la duración, cantidad de licencias y fecha de vencimiento.

IV. PLAZO DE EJECUCION DEL SERVICIO

Las licencias deberán ejecutarse en el plazo de 1 año, contados a partir del día siguiente de la entrega de la orden de servicio.

El plazo de entrega es de hasta 10 días calendarios, contado a partir del día siguiente de la entrega de la orden de servicio.

VI. CONFORMIDAD DEL SERVICIO

Para efecto del trámite de pago, la División de Procesos y Tecnología 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.

A. EXPERIENCIA DEL POSTOR — MÁXIMO 80.00 PUNTOS

Anexo N° 08 La experiencia se calificará considerando el monto facturado acumulado por el postor por prestaciones iguales o similares al objeto de la convocatoria, durante el período de ocho (08) años a la fecha de presentación de la propuesta, por un monto máximo acumulado de hasta cinco (5) Veces el valor referencial.

Tal experiencia se acreditará mediante contratos y su respectiva conformidad o mediante comprobantes de pago cuya cancelación se acredite documental y fehacientemente (el postor podrá presentar entre otros: voucher de depósito, reporte de estado de cuenta o que la cancelación conste en el mismo documento), prestados a uno o más clientes, sin establecer limitaciones por el monto o el tiempo de cada contratación que se pretenda acreditar. Los comprobantes de pago y/o contratos que se presenten deberán acreditar experiencia en **Suscripción para la solución de seguridad, antivirus, anti spam y filtro web o similares.**

La asignación de puntaje será de acuerdo al siguiente criterio:

FACTORES REFERIDOS AL POSTOR	Puntos
CRITERIO	
• Monto acumulado igual o mayor a 5 veces el valor referencial	80.00
• Monto acumulado igual o mayor a 3 veces el valor referencial y menor a 5 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

B. CAPACITACIÓN RESPECTO AL USO DE LAS SOLUCIONES — MÁXIMO 20.00 PUNTOS

El postor deberá ofrecer el servicio de capacitación sobre el uso adecuado de las soluciones de seguridad ofertadas (licencias de seguridad para Endpoint, Filtro de Mensajería y Filtro de Contenidos) para cinco (5) trabajadores del Banco, quienes serán designados posteriormente por la División de Procesos y Tecnología.

La asignación del puntaje se dará, aplicándose la siguiente escala:

CRITERIO	
• Capacitación virtual sobre el uso adecuado de las soluciones de seguridad ofertadas (licencias de seguridad para Endpoint, Filtro de Mensajería y Filtro de Contenidos) para cinco (5) trabajadores del Banco.	Puntaje 20.00
• No ofrece capacitación.	00.00

Para este factor se considera que las capacitaciones ofrecidas serán de manera virtual y tendrán una duración mínima de 06 horas en total, las cuales deberán ser distribuidas en 1 sesión de 2 horas, como mínimo, por cada solución ofertada.

No se otorgará puntaje al postor que no ofrezca capacitación.

A efectos de asignar puntaje, deberá enviar una Declaración Jurada señalando la capacitación ofrecida **(Anexo 09).**

PARA ACCEDER A LA ETAPA DE EVALUACIÓN ECONÓMICA, EL POSTOR DEBERÁ OBTENER UN PUNTAJE TÉCNICO MÍNIMO DE OCHENTA (80.00) 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 010-2021-AGROBANCO "Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"**

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 _____ del 2021

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

ANEXO N° 01

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"
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 SERVICIO CONVOCADO

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"
Presente.-

De nuestra consideración:
El que suscribe, …… (postor y/o Representante Legal) de la empresa: ....., 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 Banco Agropecuario- Agrobanco y conocer todas las condiciones existentes, el suscrito señala que el servicio ofrecido cumple con los términos de referencia, de conformidad a lo solicitado 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 cumplir con la contratación de conformidad 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
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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 Nº010-2021**, para la Suscripción para la solución de seguridad, 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.

4.- La ausencia de un conflicto de interés, de acuerdo a lo establecido en el Código de Ética y Conducta de Agrobanco, al cual me adhiero en lo que sea aplicable en mi calidad de proveedor.

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
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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 010-2021**, 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 EJECUCIÓN

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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 servicio objeto del presente proceso en el plazo de 1 año, de conformidad con lo descrito en los Términos de Referencia del Capítulo III.

Ciudad y fecha, ……

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

ANEXO Nº 06

DECLARACIÓN JURADA DE GARANTÍA TÉCNICA

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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 01 año de garantía por el servicio (MINIMO), garantizando plenamente que serán suministrado nuevos, libres de defectos de material o de producción, además se brindará la última versión de las soluciones ofertadas, que cumplirán con todas las especificaciones establecidas así como comunicación de novedades para el crecimiento .

Ciudad y fecha, ……

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

ANEXO Nº 07

DECLARACIÓN JURADA DE SERVICIO DE SOPORTE

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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 servicio de soporte técnico durante los 365 días del año.

Ciudad y fecha, ……

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

ANEXO N° 08

EXPERIENCIA DEL POSTOR

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

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					
11					
12					
13					
14					
TOTAL					

Ciudad y fecha, ……

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

ANEXO N° 09

DECLARACION JURADA DE CAPACITACIÓN

Señores
COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

Presente.-

De nuestra consideración:

Por medio de la presente, el que suscribe, don ……, Representante Legal de……..……., en su calidad de postor del proceso de selección de la referencia, DECLARA BAJO JURAMENTO ante el Banco Agropecuario –AGROBANCO lo siguiente:

1. CAPACITACIÓN OFRECIDA:

Marcar con un Aspa la Opción a Ofrecer	**Mejora**
	Capacitación virtual sobre el uso adecuado de las soluciones de seguridad ofertadas (licencias de seguridad para Endpoint, Filtro de Mensajería y Filtro de Contenidos) para cinco (5) trabajadores del Banco.
	No ofrece el servicio de capacitación.

2. Nos comprometemos a cumplir las capacitaciones ofrecidas, las cuales son de nuestra exclusiva responsabilidad y libre de costo para AGROBANCO. Asimismo, señalamos que las capacitaciones ofrecidas serán de manera virtual y tendrán una duración mínima de 06 horas en total, las cuales serán distribuidas en 1 sesión de 2 horas, como mínimo, por cada solución ofertada.

3. Nos comprometemos a entregar un certificado a cada participante por la capacitación brindada.

Atentamente,

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

ANEXO Nº 10

CARTA DE PROPUESTA ECONÓMICA

(MODELO)

Señores

COMITÉ DE ADQUISICIONES NIVEL I
ADQUISICION DE NIVEL I Nº 010-2021-AGROBANCO
"Suscripción para la Solución de Seguridad, Antivirus, Antispam y Filtro Web"

Presente.-

De nuestra consideración,

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

CANT.	CONCEPTO (indicar marca y versión)	PRECIO UNITARIO S/.	PRECIO TOTAL S/.
	Total		

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