BASES

ADQUISICIÓN NIVEL II Nº0024-2024-AGROBANCO

"ADQUISICIÓN DE LICENCIAS ANTISPAM Y ANTIVIRUS"

2024

SECCIÓN GENERAL

DISPOSICIONES COMUNES A TODOS LOS NIVELES DE CONTRATACIÓN

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 Contrataciones de AGROBANCO, publicado en la página web de Agrobanco.
- Manual de Procedimientos de Contrataciones de AGROBANCO, publicado en la página web del Agrobanco.
- Política de Contrataciones de AGROBANCO, publicado en la página web de Agrobanco.

a) <u>De la Convocatoria del proceso de Adquisición</u>

- La convocatoria de todo Procedimiento de Selección se realizará a través de la página web conteniendo la aprobación del Expediente de Contratación, las Bases y la aprobación de las Bases; e invitación directa por correo electrónico a todos los potenciales proveedores de bienes y servicios, adjuntando las Bases[1].

- Para dar inicio al Procedimiento de Selección, la División de Logística apoya al Comité de Selección, gestionando la convocatoria en base al calendario aprobado y realiza la invitación a un mínimo de dos (02) empresas, incluyendo a las que participaron en el estudio de mercado.

- La publicación de las bases y el registro del procedimiento de selección hasta la Buena Pro o Declaratoria de Desierto, a efecto que el público en general tenga acceso en forma gratuita, se realizará en la página web del Banco y en el Portal de Transparencia Estándar.

- Durante el desarrollo del procedimiento de selección y en caso se recepcione una sola oferta o cuando exista una sola oferta válida, previa conformidad vía correo electrónico del Gerente de Administración, Operaciones y Finanzas, el Comité de Selección podrá continuar con el procedimiento de selección y otorgar la buena pro, siempre que cumpla con todos los requisitos exigidos en las bases.

[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 021-2019-JUS.

b) <u>Del Registro de Participantes y plazos de los procedimientos de selección</u>

- Efectuada la convocatoria, las empresas deberán registrarse obligatoriamente y de forma gratuita, a fin de poder participar en el proceso, adjuntando copia del Registro Nacional de Proveedores vigente emitido por la OSCE. Este registro podrá ser por medio electrónico o físico, conforme a lo establecido en las Bases.

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

NIVEL	N° DE INVITACIONES	PLAZOS
Nivel IV	Mínimo 2	Desde convocatoria hasta recepción de ofertas: Mínimo 11 días hábiles. Desde presentación de ofertas hasta Buena Pro: Mínimo 4 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 5 días hábiles. Desde consentimiento, hasta la suscripción del contrato: Mínimo 3 días hábiles.
Nivel III	Mínimo 2	Desde convocatoria hasta recepción de ofertas: Mínimo 10 días hábiles. Desde presentación de ofertas hasta Buena Pro: Mínimo 3 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 4 días hábiles. Desde consentimiento, hasta la suscripción del contrato: Mínimo 3 días hábiles.
Nivel II	Mínimo 2	Desde convocatoria hasta recepción de ofertas: Mínimo 8 días hábiles. Desde presentación de ofertas hasta Buena Pro: Mínimo 2 días hábiles. Desde Buena Pro hasta consentimiento: Mínimo 2 días hábiles. Desde consentimiento, hasta la suscripción del contrato: Mínimo 3 días hábiles.
Nivel I	Mínimo 2	Desde convocatoria hasta recepción de ofertas: Mínimo 2 días hábiles. Desde presentación de ofertas 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.

- Durante el desarrollo del procedimiento de selección y en caso se recepcione una sola oferta o cuando exista una sola oferta válida, previa conformidad vía correo electrónico del Gerente de Administración, Operaciones y Finanzas, el Comité de Selección podrá continuar con el procedimiento de selección y otorgar la buena pro, siempre que cumpla con todos los requisitos exigidos en las bases.

c) De la Formulación de consultas y observaciones

- Los procesos de nivel II y III preverán un plazo mínimo de dos (02) días hábiles posteriores a la convocatoria, para que los participantes formulen consultas y observaciones, y un plazo máximo de tres (03) días hábiles para que el Comité de Selección emita el Acta de absolución de consultas y observaciones y otras acciones que se consideren de utilidad para obtener ofertas que cumplan con las condiciones indicadas. Solo en los procesos de Nivel IV, se preverán un plazo mínimo de tres (03) días hábiles posteriores a la convocatoria, para que los participantes formulen consultas y observaciones y un plazo máximo de tres (03) días hábiles para que el Comité

de Selección emita el Acta de absolución de consultas y observaciones. Estas fechas y modalidad de presentación estarán incluidas en las bases.

- Mediante las consultas, para el caso de los niveles II, III y IV, 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 la vulneración de las bases a la normativa aplicable al Procedimiento de Selección u otra normativa que tenga relación con el objeto de la contratación. Esta etapa podrá realizarse por medio electrónico.

d) De la Absolución de consultas y observaciones e Integración de Bases

- El Comité de Selección absolverá las consultas y observaciones mediante un mismo pliego absolutorio, debidamente fundamentado, el que deberá contener la identificación de cada participante que formuló las consultas y/u observaciones presentadas, así como las respuestas a cada una de ellas, procediendo luego a integrar las Bases.

- 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. En esta etapa, el Banco podrá realizar mayor precisión o aclaración respecto de las Bases, indistintamente si se hubieran presentado consultas u observaciones.

- 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.

- El plazo mínimo entre la absolución de consultas y la presentación de oferta es de tres (03) días hábiles.

e) Recepción de Ofertas

- Los tiempos mínimos para la presentación de la oferta por parte del postor, el otorgamiento de la Buena Pro, el consentimiento y suscripción del contrato será de acuerdo a lo establecido en el Reglamento de Contrataciones de AGROBANCO.

- La recepción de las ofertas 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 o medio electrónico que se indique en las Bases. Para que una oferta sea admitida deberá incluir la documentación de presentación obligatoria que se establezca en las bases.

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

- En los Procedimientos de Selección correspondientes a los niveles "II", "III" y "IV", la recepción de ofertas y otorgamiento de la buena pro se efectuará en acto público en presencia de un notario público, en el caso del nivel "I" de contratación dichos actos serán privados.

- Cuando se trate de un acto público de presentación de ofertas, este 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 Procedimiento de Selección, para que entreguen sus ofertas. El Comité de Selección procederá a abrir los sobres que contienen la oferta técnica de cada postor y comprobará que los documentos presentados por cada postor sean los solicitados por las Bases Integradas. De no ser así, devolverá la oferta, teniéndola por no presentada. Si las Bases Integradas han previsto que la evaluación y calificación de las ofertas técnicas se realice en fecha posterior, el notario procederá a colocar los sobres cerrados de las ofertas económicas de todos los postores, dentro de uno o más sobres, los que serán debidamente sellados y firmados por él, conservándolos hasta la fecha en que el Comité de Selección, en acto público, comunique verbalmente a los postores el resultado de la evaluación de las ofertas técnicas.

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

- 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 o debidamente apostillados, en caso sea favorecido con la Buena Pro.

- Constituyen documentos de presentación obligatoria:

  a. Copia Simple de la Constancia de Inscripción vigente en el Registro Nacional de Proveedores.
  b. Formulario de Declaración Jurada de Proveedores y Contrapartes, el cual será remitido a la Oficialía de Cumplimiento para su revisión en las bases y/o Listas internas, externas e internacionales que se encuentran del Manual PLAFT.
  c. Formatos solicitados en las Bases como documentación de presentación obligatoria.
  d. 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.

  La Declaración Jurada de Proveedores y Contrapartes deberá incluir los nombres y apellidos completos y tipo y número de documento de identidad en caso se trate de persona natural o razón social en caso se trate de una persona jurídica. Debiendo contener además la identificación de los accionistas, socios o asociados que tengan directa o indirectamente capital social o participación de la persona jurídica y el nombre del representante legal, asimismo deberá señalar en esta declaración jurada los antecedentes penales del personal consignado.

- Constituyen documentos de presentación facultativa:
  Documentación que sustente el cumplimiento de los factores de evaluación.

- Las ofertas presentadas deberán adjuntar una Declaración Jurada conteniendo lo siguiente:

  a. No haber incurrido y se obliga a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
  b. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado.

c. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

d. Conocer, aceptar y someterse a las bases, condiciones y reglas del procedimiento de selección.

e. Ser responsable de la veracidad de los documentos e información que presente en el procedimiento de selección.

f. No haber tenido ningún vínculo laboral con el Banco en los últimos 12 meses.

g. Comprometerse a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

h. La ausencia de conflicto de interés, de acuerdo a lo establecido en el Código de Ética y Conducta de AGROBANCO, al cual se adhiere en lo que sea aplicable en su calidad de proveedor.

i. Actualmente, no está siendo investigado y/o procesado (o lo estuvo anteriormente), por el delito de lavado de activos, financiamiento del terrorismo y/o delito precedente.

- Todos los documentos que contengan información referida a los requisitos para la admisión de ofertas 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.

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

- Las ofertas 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 o servicio a adquirir o contratar; excepto la de aquellos postores que gocen de exoneraciones legales. El monto de la oferta económica y los subtotales que componen serán expresados con dos decimales. La oferta económica deberá encontrarse debidamente suscrita por el representante legal, de lo contrario quedará descalificada.

- Si existieran defectos de forma, tales como errores u omisiones subsanables en los documentos presentados que no modifiquen el alcance de la oferta técnica, el Comité de Selección podrá solicitar la subsanación y otorgará un plazo entre uno (1) o dos (2) días hábiles, desde el día de la notificación de los mismos, para que el postor los subsane, en cuyo caso la oferta 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. En los casos que la revisión del Formulario de Declaración Jurada de Proveedores y Contrapartes presente alguna observación de forma o contenido realizada por la Oficialía de Cumplimiento, podrá ser sujeta a subsanación.

- Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio en un procedimiento de selección, o en un determinado ítem cuando se trate de procesos de selección según relación de ítems.

- 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 estará a cargo de la Gerencia Legal y Cumplimiento Normativo y será informado vía correo electrónico a la División de Logística en un plazo máximo de 1 día hábil y 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 no admitir la oferta.

f) De la Evaluación de Ofertas

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

- En todos los procedimientos de selección, durante la evaluación del expediente técnico, la Oficialía de Cumplimiento deberá informar vía correo electrónico el resultado de su revisión en las bases y/o Listas negativas de todos los postores que presentaron oferta. El resultado deberá ser informado a la División de Logística en el plazo máximo de un (01) día hábil. En los casos que los proveedores no pasen esta revisión se procederá a no admitir la oferta.

- Solo una vez admitidas las ofertas, el Comité de Selección 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 ofertas que en la evaluación técnica alcancen el puntaje mínimo fijado en las Bases, accederán a la evaluación económica. Las ofertas técnicas que no alcancen dicho puntaje serán descalificadas en esta etapa.

- El Comité de Selección incluirá en las bases los criterios que utilizará para evaluar las ofertas, el puntaje que asignará a cada uno de estos criterios y precisará que 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.

- La asignación del puntaje otorgado a los postores por la acreditación del cumplimiento de cada criterio de evaluación, será decisión del Comité de Selección.

- La oferta 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 o servicio a adquirir o contratar.

- Criterios de evaluación
  - Se establecerán criterios o factores de evaluación para cada procedimiento de selección.

A. Factores de evaluación para la contratación de bienes.

En caso de contratación de bienes podrán considerarse los siguientes factores de evaluación de la oferta técnica, según corresponda al tipo del bien, su naturaleza, finalidad, funcionalidad y a la necesidad del Banco:

- El plazo de entrega.
- La garantía comercial del postor o del fabricante.
- La disponibilidad de servicios y repuestos.
- La capacitación del personal del Banco.
- Mejoras a las especificaciones técnicas de los bienes y a las condiciones previstas en las Bases, que no generen costo adicional para el Banco. Las Bases deberán precisar aquellos aspectos que serán considerados como mejoras.
- La experiencia del postor, la cual se calificará considerando el monto facturado acumulado por el postor durante un período determinado de hasta ocho (8) años a la fecha de la presentación de ofertas, por un monto máximo acumulado de hasta cuatro (4) veces el valor referencial de la contratación o ítem materia de la convocatoria, sin que las Bases puedan establecer limitaciones referidas a la cantidad, monto o a la duración de cada contratación que se pretenda acreditar.
- La experiencia se acreditará sin importar el número de documentos que la sustenten. Tal experiencia se acreditará mediante contratos, órdenes de compra y su respectiva conformidad por la venta o suministro efectuados; o mediante comprobantes de pago cuya cancelación se acredite documental y fehacientemente. En el caso de suministro de bienes, sólo se considerará la parte que haya sido ejecutada hasta la fecha de presentación de ofertas, debiendo adjuntar la conformidad de la misma o acreditar su pago.
- El Comité de Selección podrá establecer otros factores de evaluación relacionados al objeto de la convocatoria.

B. Factores de evaluación para la contratación de servicios en general

- En caso de contratación de servicios en general deberá considerarse como factor referido al postor la experiencia, en la que se calificará la ejecución de servicios en la actividad y/o en la especialidad, considerando el monto facturado acumulado por el postor durante un período determinado de hasta ocho (08) años a la fecha de la presentación de ofertas, por un monto máximo acumulado de hasta cuatro (04) veces el valor referencial de la contratación o ítem materia de la convocatoria.
- Se acreditará mediante contratos u órdenes de servicio y la respectiva conformidad por la prestación efectuada o mediante comprobantes de pago cuya cancelación se acredite documental y fehacientemente, sin establecer limitaciones por el monto o el tiempo de cada servicio que se pretenda acreditar. En el caso de servicios de ejecución periódica, sólo se considerará la parte que haya sido ejecutada hasta la fecha de presentación de ofertas, debiendo adjuntar la conformidad de la misma o acreditar su pago

Adicionalmente, podrán considerarse los siguientes factores de evaluación de la oferta técnica, según corresponda al tipo del servicio, su naturaleza, finalidad y a la necesidad del Banco:

- Personal propuesto para la prestación del servicio, el cual se evaluará por el tiempo de experiencia en la especialidad del personal propuesto para la ejecución del servicio, que se acreditará con constancias o certificados También se considerará capacitaciones o conocimientos adquiridos del personal propuesto, relacionados al objeto de la convocatoria.
- Mejoras a las condiciones previstas. Las bases deberán precisar aquellos aspectos que serán considerados como mejoras.
- Otros factores referidos al objeto de la convocatoria tales como equipamiento, infraestructura.
- En el supuesto que el postor fuera una persona natural, la experiencia que acredite como tal, podrá acreditarla también como personal propuesto para el servicio, si fuera el caso.
- El Comité de Selección podrá establecer otros factores de evaluación relacionados al objeto de la convocatoria.
- El único factor de evaluación de la oferta económica será el monto total indicado en la misma, debiendo estar suscrito por el representante legal.

g) Evaluación

- La calificación y evaluación de las ofertas es integral, realizándose en dos (02) etapas. La primera es la técnica, cuya finalidad es calificar y evaluar la oferta técnica, y la segunda es la económica, cuyo objeto es calificar y evaluar el monto de la oferta.

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

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

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

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

Donde:

i = Oferta
Pi = Puntaje de la oferta económica a evaluar
Oi = Precio de la oferta económica i.
Om = Precio de la oferta económica más baja.
PMP= Puntaje máximo dela oferta económica.

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

  - Etapa de evaluación técnica:

- ✓ El Comité de Selección evaluará cada oferta de acuerdo con las Bases y conforme a una escala que sumará cien (100) puntos.
- ✓ Para acceder a la evaluación de las ofertas económicas, las ofertas 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 ofertas técnicas que no alcancen dicho puntaje serán descalificadas en esta etapa.

• Etapa de evaluación económica:

El puntaje de la oferta económica se calculará siguiendo las pautas señaladas, donde el puntaje máximo para la oferta económica será de cien (100) puntos. Las ofertas que superen el valor referencial serán descalificadas.

• Determinación del puntaje total:

- ✓ Una vez evaluadas las ofertas 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 oferta 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:

- ✓ La suma de ambos coeficientes deberá ser igual a la unidad (1.00).
- ✓ Los valores que se aplicarán en cada caso deberán estar comprendidos dentro de los márgenes siguientes:

En todos los casos de contrataciones aplicarán las siguientes ponderaciones:

$$0.60 < c1 < 0.70; \text{ y } 0.30 < c2 < 0.40$$

- La oferta evaluada como la mejor será la que obtenga el mayor puntaje total.
- Los miembros del Comité de Selección no tendrán acceso ni evaluarán las ofertas económicas, sino hasta que la evaluación técnica haya concluido.
- A efectos de la admisión de la oferta económica, el Comité de Selección verificará que el monto ofertado no exceda el valor referencial, pudiendo el postor ofertar por debajo de este. Las ofertas que excedan del valor referencial serán descalificadas. En caso se verifique que una oferta económica no se encuentra debidamente firmada por el representante legal será descalificada.
- La labor del Comité de Selección concluye con el consentimiento de la Buena Pro, entregando el Expediente de Contratación a la División de Logística.
- La División de Logística comunicará al postor ganador la Buena Pro, y solicitará la documentación pertinente para perfeccionar el contrato u orden según cada

caso; y, gestionará el envío de la orden de compra u orden de servicio, o procederá a la suscripción del contrato respectivo.

h) De la Buena Pro

- El Comité de Selección otorgará la buena pro al postor que haya obtenido el mayor puntaje. En los procesos correspondientes a los niveles II, III y IV, 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 nivel I, 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 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 y servicios. En el caso de la suscripción de un contrato, este quedará perfeccionado cuando el Banco y el representante legal del postor suscriban el documento que lo contiene.

- Cuando no se presente ninguna oferta o no quede ninguna oferta válida, se declarará desierto el proceso de selección. El Comité de Selección deberá establecer en el acta de desierto los motivos que originaron el mismo. La declaratoria de desierto se publicará en la página web del Banco.

- En caso de no interponerse apelación dentro de los plazos indicados en el numeral 7.3.6 del Reglamento de Contrataciones de AGROBANCO, esta quedará consentida, y se procederá a emitir la orden de compra, de servicio o contrato, según corresponda. En aquellos supuestos, en los cuales solo se hubiese presentado un postor, se podrá emitir la orden de compra, de servicio o suscribir el contrato, de manera inmediata, previa remisión de la documentación solicitada en las bases, de ser el caso.

- Una vez otorgada la Buena Pro, la División de Logística solicitará a la División de Recursos Humanos la evaluación de conflicto de interés de la empresa adjudicada con la Buena Pro, a través del envío de la Declaración Jurada de Proveedores y Contrapartes presentada por el proveedor, documento que tiene el listado de sus representantes legales. La respuesta de la División de Recursos Humanos será dentro del plazo de dos (02) días hábiles para los Niveles I y II y tres (03) días hábiles para los Niveles III y IV. En los casos que se determine que la empresa ganadora cuenta con algún conflicto de interés, se procederá a Dejar sin Efecto de la Buena Pro, con la consiguiente notificación notarial al proveedor indicando la causal que lo motivó.

- Si por responsabilidad del postor ganador se dejara sin efecto la Buena Pro otorgada, el Comité de Selección procederá a otorgar la buena pro al postor que quedó en segundo lugar; en caso no exista ninguna oferta válida en segundo lugar, se procederá a declarar desierto el procedimiento de selección.

- En caso de declararse desierto un proceso de selección perteneciente a los Niveles II, III y IV, 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 ofertas.

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

- Asimismo, el expediente de contratación deberá contar con el correo y/o reporte que sustente la revisión efectuada por la Oficialía de Cumplimiento, en las bases y/o Listas negativas, indicadas en el Manual de Prevención de Lavado de Activos y el Financiamiento del Terrorismo.

i) <u>De la Generación de Orden de Compra, Orden de Servicio o Suscripción del Contrato</u>

- El resultado de la Bueno Pro consentida se traduce en un documento formal que incluye las condiciones del acuerdo de 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 bien o servicio, precio, plazo de entrega, el contrato se perfecciona con la suscripción del documento que lo contiene o con la notificación de la orden de compra o de servicios, para la suscripción del contrato, este deberá, ser suscrito tanto por el Banco como por el contratista. En las contrataciones cuyo monto correspondan al nivel I, el contrato podrá perfeccionarse con la notificación de la respectiva orden de compra u orden de servicio al proveedor. Forma parte del contrato el documento que lo contiene, las bases, las ofertas y los documentos derivados del procedimiento de selección que establezca obligaciones para las partes.

- La vigencia del contrato será desde su perfeccionamiento, con la notificación de la orden de compra o de servicio, o de la suscripción del documento que lo contiene, hasta la conformidad y pago de la última prestación, en caso de bienes y servicios, y hasta el consentimiento de la liquidación y se efectúe el pago correspondiente.

- Las órdenes de compra o servicio de las compras menores o iguales a cinco (05) UIT, deberán contener como mínimo: Descripción del bien o servicio a contratar, precio, plazo de entrega del bien o prestación del servicio.

- Para el caso de contratos, se utilizará el modelo de contrato estandarizado incluido en las Bases, tanto para bienes como servicios, y será revisado por la Gerencia de Legal y de Cumplimiento Normativo.

- Para las compras menores o iguales a cinco (05) UIT, la División de Logística emitirá la orden de compra o servicios, según corresponda. Además culminado el mes en curso, la División de Logística deberá publicar en la página web del Banco el reporte de órdenes de compra y servicio aprobadas dentro de los primeros 7 días hábiles del mes siguiente. El reporte deberá contener la descripción de la contratación, monto, proveedor contratado, plazo y fecha de la orden.

- Asimismo, las órdenes de compra y servicio menores o iguales a 5 UIT aprobadas, que genere el Banco, se registrarán en el SEACE, siendo el plazo máximo de publicación de 5 días hábiles del mes siguiente. El registro de información debe consignar lo siguiente: Datos de la Entidad contratante, descripción de la contratación, monto total, y Datos del contratista. Además el reporte mensual de estas órdenes aprobadas deberá ser publicado en el Portal de Transparencia Estándar, sujeto a los plazos previstos en la Circular de Transparencia del Banco.

- En todos los Niveles de Selección, el plazo máximo para la emisión de la Orden o la suscripción del Contrato es de diez (10) días hábiles, luego de que la Buena Pro quede consentida. El Banco podrá otorgar un plazo adicional para subsanar los requisitos para el perfeccionamiento del contrato, el que no podrá exceder de cinco (05) días hábiles contados desde el día siguiente de la notificación.

- La firma de todo documento oficial dirigido a un postor, en cualquier etapa del procedimiento de selección, residirá en la Gerencia de Administración, Operaciones y Finanzas o en la División de Logística.

- Documentación mínima para suscripción de contrato o generación de orden, Nivel I:

  - ✓ Copia de DNI del Representante Legal.
  - ✓ Copia de la vigencia del poder del representante legal de la empresa no mayor a sesenta (60) días de antigüedad.
  - ✓ Copia del Testimonio 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.
  - ✓ Copia del RUC (Registro Único de Contribuyente), o registro equivalente para no domiciliados, de ser el caso. Debiendo incluir la fecha de inicio de actividades y los rubros en los que el proveedor brinda sus productos o servicios.
  - ✓ Declaración jurada consignando dirección de la oficina o local principal para efectos de notificación u otros fines.
  - ✓ Contrato de consorcio con firmas legalizadas de los consorciados, de ser el caso.
  - ✓ Número de cuenta o Código de Cuenta Interbancario (CCI), de corresponder.
  - ✓ Otra documentación que sea necesaria para el cumplimiento de la contratación.

- Documentación mínima para suscripción de contrato, Nivel II, III y IV:

  Adicionalmente a los requisitos indicados en el párrafo anterior, se añaden los siguientes:
  - ✓ Garantía de fiel cumplimiento de contrato, de ser el caso.
  - ✓ Otra documentación que sea necesaria para el cumplimiento de la contratación.

J) 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, sin beneficio de excusión y de realización automática en el país, al sólo requerimiento de Agrobanco. Se establecen los siguientes tipos de garantía.

a. Garantía por Adelanto

- El Banco sólo puede entregar los adelantos previstos en las Bases contra la presentación de una garantía emitida por un idéntico monto y un plazo mínimo de vigencia de tres (03) 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 (03) 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 y de materiales 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.

b. Garantía por Fiel Cumplimiento

Como requisito indispensable para suscribir el contrato, a partir de sesenta (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 contratista, en el caso de bienes y servicios.

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 se ejecutará, en su totalidad, sólo cuando la resolución invocada por Agrobanco por causa imputable al contratista ha quedado consentida, o cuando por laudo arbitral consentido se declare procedente la decisión de resolver el contrato. El monto de las garantías corresponderá íntegramente al Banco, independientemente de la cuantificación del daño efectivamente irrogado.
- Igualmente, la garantía de fiel cumplimiento se ejecutarán cuando transcurridos tres (03) 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. Esta ejecución será solicitada por un monto equivalente al citado saldo a cargo del contratista.

CAPÍTULO II

PERFECCIONAMIENTO DEL CONTRATO

a) <u>De los contratos y su ejecución</u>

- Los contratos deben incluir las cláusulas mínimas exigidas y precisadas en el Reglamento de Contrataciones de AGROBANCO.
- La División de Logística enviará a la Gerencia de Legal y Cumplimiento Normativo el proyecto de contrato u documentos para formalización de la orden y los documentos enviados por el Contratista (Ficha RUC, Vigencia de Poder actualizada, Testimonios de Constitución y modificación, copia de la Carta Fianza, Declaración Jurada consignando dirección de local, entre otros detallados en las Bases), a fin de que la Gerencia de Legal y Cumplimiento Normativo revise y otorgue su conformidad a los datos consignados en el contrato y los documentos.

- La División de Logística remitirá el original de la Carta Fianza a la División de Operaciones, quien solicitará mediante correo electrónico, página web o vía telefónica al Banco emisor la confirmación de la validez de las Cartas Fianzas entregadas al Banco por el postor ganador; posteriormente la Carta Fianza (documento original) deberá ser archivado y custodiado.

- La División de Operaciones es responsable de realizar el monitoreo de la vigencia de las Cartas Fianzas entregadas al Banco por el postor ganador, informando a la División de Logística el vencimiento de las mismas para los trámites que correspondan.

- De conformidad con el numeral 5.3.3 del presente Manual de Contrataciones, es responsabilidad de las unidades usuarias velar por el efectivo cumplimiento de los términos de referencia y/o especificaciones técnicas a fin de asegurar que la ejecución de los contratos, órdenes de compra y/o servicio, se efectúe de acuerdo a lo requerido. Asimismo, para aquellos factores de evaluación que prevalezcan durante la ejecución contractual, la verificación de su cumplimiento deberá realizarlo el analista o asistente de la División de Logística, en conjunto con la unidad usuaria a quien se les brinda el servicio.

- Además del Documento Nacional de Identidad para los ciudadanos nacionales, se considerarán documentos válidos para la celebración de contratos, respecto a ciudadanos extranjeros con calidad migratoria de residente, el Pasaporte, el Carnet de Identidad emitido por el Ministerio de Relaciones Exteriores, el carnet del Permiso Temporal de Trabajo (PTP) o carnet de Permiso Temporal de Permanencia, el carnet de Extranjería y en ambos casos, las constancias que acreditan su tramitación de acuerdo a lo dispuesto por Migraciones, asimismo, la Cédula de Identidad o documentos análogos, el Carnet del Refugiado y el Documento expedido por la CEPR del Ministerio de Relaciones Exteriores que acredita que la solicitud de refugiado se encuentra en trámite.

b) <u>De la Recepción y Conformidad de Bienes y Servicios</u>

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

- Se verificará que lo recibido sea de acuerdo a lo solicitado por la unidad usuaria, siendo responsable la Gerencia Usuaria o quien haga sus veces.

- Ninguna Gerencia podrá otorgar la conformidad de una prestación, sin tener certeza que el proveedor culminó con la totalidad de trabajos indicados en los términos de referencia o especificaciones técnicas, quedando la contratación a satisfacción del área usuaria solicitante.

- El informe de conformidad se emite en un plazo máximo de diez (10) días hábiles de producida la recepción y previa recepción de la factura o comprobante de pago. Dependiendo de la complejidad o sofisticación de la contratación, la conformidad se podrá emitir en un plazo máximo de quince (15) días hábiles.

- De existir observaciones se consignarán en el acta respectiva, indicándose claramente el sentido de éstas, dándose al contratista un plazo prudencial para su subsanación, en función a la complejidad del servicio. Dicho plazo no podrá ser menor de dos (02) ni mayor de diez (10) días hábiles. Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la Entidad podrá resolver el contrato, sin perjuicio de aplicar las penalidades que correspondan.

- En el caso de servicios, el área usuaria solicitante otorgará la conformidad del servicio y en el caso de bienes, la validación será realizada conjuntamente con el encargado del almacén a través de la recepción de la guía de remisión o quien haga sus veces con la unidad usuaria; respetando lo establecido en el procedimiento de almacenamiento de bienes.

- Para las compras menores o iguales a cinco (05) UIT y contrataciones correspondientes a los Niveles I, II, III y IV, el área usuaria solicitante deberá inspeccionar y aprobar técnicamente la entrega del bien o el servicio prestado, verificando que se haya realizado conforme a las especificaciones técnicas o términos de referencia y condiciones contratadas, debiendo emitir la conformidad respectiva de la entrega del bien o el servicio prestado.

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

c) Del Expediente de Compra

Los procesos de compra mantendrán para su control un expediente de compras, el cual mantendrá un orden y conservará los tipos de documentos en función al tipo de proceso realizado. El expediente contendrá como mínimo la siguiente documentación, de acuerdo al tipo de proceso:

- **Compras menores o iguales a cinco (05) UIT**
  - ✓ Requerimiento, incluyendo los términos de referencia o especificaciones técnicas.
  - ✓ Cotización.
  - ✓ Orden de compra o servicio, previa disponibilidad presupuestal.
  - ✓ Conformidad de la contratación.

- **Compras mayores a cinco (05) UIT**
  - ✓ Requerimiento, incluyendo los términos de referencia o especificaciones técnicas.
  - ✓ Estudio de posibilidades que ofrece el mercado (cotizaciones, de acuerdo al mínimo requerido).
  - ✓ Aprobación del expediente de la contratación.
  - ✓ Bases y aprobación de las bases.
  - ✓ oferta de los postores.
  - ✓ Acta de Buena pro.
  - ✓ Orden de compra, servicio o contrato.
  - ✓ Conformidad de la contratación.

d) Del Registro de Proveedores

La División de Logística es la unidad encargada de mantener un registro de proveedores actualizado, el cual estará ingresado en el sistema administrativo.

e) De las contrataciones adicionales, complementarias o reducciones

Para las contrataciones complementarias, prestaciones adicionales y reducciones, de los niveles I, II, III y IV; estas deberán ser solicitadas por las unidades usuarias, debiendo ser aprobadas por la Gerencia de Administración, Operaciones y Finanzas, siendo formalizadas a través de un Acta con la participación de la División de Logística.

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 para la **ADQUISICIÓN DE LICENCIAS ANTISPAM Y ANTIVIRUS.**

2. VALOR REFERENCIAL

El valor referencial asciende **S/ 440,000.00** (Cuatrocientos Cuarenta Mil con 00/100 Soles), incluido los impuestos de Ley y cualquier otro concepto que incida en el costo total del bien. El valor referencial ha sido calculado al mes de noviembre del 2024.

3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante documento de fecha XX de noviembre del 2024.

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

Esta Adquisición se encuentra definido en el Capítulo III de la presente sección.

6. PLAZO DE ENTREGA

El plazo de entrega de los bienes objeto de la contratación, tendrá los siguientes plazos:

Etapa 1: El plazo de entrega de las licencias será de hasta quince (15) días calendario, contado a partir del día siguiente de la firma del contrato.

Etapa 2: El plazo máximo para realizar la implementación de la solución se realizará hasta los sesenta (60) días calendarios contados a partir de la conformidad de la etapa 1.

La activación de las licencias será culminada el periodo de Instalación, configuración y puesta en producción de las soluciones ofertadas.

Etapa 3: El plazo de esta etapa de operación es de 12 meses que dura el contrato.

CAPÍTULO II

DEL PROCESO DE SELECCIÓN

1. CRONOGRAMA DEL PROCESO DE SELECCIÓN

Actividades	Fecha	
	Desde	Hasta
Convocatoria	16/12/2024	
Registro de Participantes	17/12/2024	27/12/2024
Presentación de consultas y observaciones Se presentarán electrónicamente a los correos: **amezones@agrobanco.com.pe.** En el horario de 09:00 a 18:00 horas. No se aceptará ninguna consulta fuera de la fecha y horario establecido.	17/12/2024	18/12/2024
Absolución de consultas y observaciones	19/12/2024	23/12/2024
Integración de Bases	24/12/2024	
Presentación de Propuestas El acto público se realizará en Av. República de Panamá 3531 Piso 9, San Isidro, a las **11:00 am.**	**30/12/2024**	
Calificación y Evaluación de Propuestas Técnicas	31/12/2024	06/01/2025
Evaluación Económica y Otorgamiento de la Buena Pro El acto público se realizará en Av. República de Panamá 3531 Piso 9, San Isidro, a las **11:00 am.**	**07/01/2025**	

2. REGISTRO DE PARTICIPANTES

El registro de los participantes se realizará **gratuitamente** de manera electrónica a los correos amezones@agrobanco.com.pe , en el horario de 09:00 a 18:00 horas en las fechas indicadas en el numeral 7 del presente capítulo (días hábiles). El participante deberá presentar el Formato Nº1 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 RNP (Bienes). La hora y fecha de recepción será la 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

Las propuestas se presentarán en acto público, en Av. República de Panamá 3531, Piso 9 - San Isidro, en la fecha y hora señalada en el cronograma. El acto público se realizará con la participación de Notario.

Las personas naturales concurrirán personalmente o a través de su apoderado debidamente acreditado ante el Comité de Adquisiciones mediante carta poder simple. Las personas jurídicas lo harán por medio de su representante legal o apoderado. El representante legal acreditará tal condición con copia simple del documento registral vigente que consigne dicho cargo y, en el caso del apoderado, será acreditado con carta poder simple suscrita por el representante legal, a la que se adjuntará el documento registral vigente que acredite la condición de éste.

Las propuestas se presentarán en dos sobres cerrados y estarán dirigidas al Comité de Adquisiciones de la **ADQUISICIÓN NIVEL II N° 024-2024-AGROBANCO,** conforme al siguiente detalle:

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

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

ADQUISICIÓN NIVEL II N°0024-2024-AGROBANCO
Objeto del proceso: "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS

SOBRE N°1: OFERTA TÉCNICA
NOMBRE / RAZON SOCIAL DEL POSTOR:
Nº DE FOLIOS:

SOBRE Nº2: Oferta Económica. El sobre será rotulado:

Señores
AGROBANCO
Av. República de Panamá 3531 – Piso 9 - San Isidro
Att.: Comité de Selección Nivel II
ADQUISICIÓN NIVEL II N°0024-2024-AGROBANCO
Objeto del proceso: "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS

SOBRE N°02: OFERTA ECONÓMICA
NOMBRE / RAZON SOCIAL DEL POSTOR:
Nº DE FOLIOS:

4. CONTENIDO DE LAS OFERTAS

SOBRE Nº1 - OFERTA 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:

- **Documento que acredite la representación de quien suscribe la oferta.**

  Copia simple del documento registral vigente del representante legal que suscribe la oferta donde conste el cargo que ocupa y las facultades para participar como postor en licitaciones o concursos públicos. En caso de no participar personalmente el representante que suscribe la oferta, deberá enviar apoderado, adjuntando carta poder simple suscrita por el representante legal, a la que se adjuntará el documento registral vigente que acredite la condición de este.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe de ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

- Copia simple de la Constancia de inscripción vigente en el Registro Nacional de Proveedores de OSCE: **Registro de Bienes.**

- Declaración Jurada de datos del postor. Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados - **Anexo Nº01.**

- Declaración jurada y/o documentación que acredite el cumplimiento de los Requerimientos Técnicos Mínimos contenidos en el Capítulo III de la presente sección - **Anexo Nº02.**

- Declaración jurada en la que se compromete a mantener la vigencia de la oferta hasta la suscripción del contrato u orden, no tener impedimentos para contratar con el Estado, no haber incurrido ni incurrir en actos de corrupción, etc., entre otros. - **Anexo Nº03.**

- Promesa de consorcio, de ser el caso, consignando los integrantes, el representante común, el domicilio común y el porcentaje de participación - **Anexo Nº04.**

  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 para proveedores y contrapartes, la cual deberá incluir los nombres y apellidos completos y tipo y número de documento de identidad en caso se trate de persona natural o razón social en caso se trate de una persona jurídica. Debiendo contener además la identificación de los accionistas, socios o asociados que tengan directa o indirectamente capital social o participación de la persona jurídica y el nombre del representante legal, asimismo deberá señalar en esta declaración jurada los antecedentes penales del personal consignado. **- Anexo Nº05**

- Declaración jurada sobre el Plazo de entrega del bien - **Anexo Nº06**

- Declaración Jurada de Garantía Anual- **Anexo Nº07**
- Declaración jurada de representación deberá ser partner de la marca ofertada, adjuntando una carta de fabricante haciendo referencia al proceso que acredite que está autorizado para comercializar licencias, mantenimiento de licencias, soporte técnico y suscripción de licencias **- Anexo N°08**
- Declaración jurada relación del personal propuesto - **Anexo N°09**
- Declaración jurada de Taller de transferencia de conocimientos **- Anexo N°10**
- Declaración jurada de soporte y mantenimiento**- Anexo N°11**
- Declaración jurada de la solución **- Anexo N°12**
- El postor deberá adjuntar la ficha técnica de las Licencias Antispam y Antivirus.
- Copia simple de la Copia Literal emitida por SUNARP y Ficha RUC del postor, mediante el cual demuestre por lo menos 5 años (o más) de estar constituido en el mercado local.

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

Documentación de presentación facultativa

- Criterios de evaluación: Experiencia del postor- **Anexo Nº13**
- Criterios de evaluación: Mejoras previstas en las bases – **Anexo N°07**

SOBRE N°2 - OFERTA ECONÓMICA

Se presentará en un (1) original.

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

- Oferta económica - **Anexo Nº14**

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

5. DETERMINACION DEL PUNTAJE TOTAL

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

El puntaje total de las ofertas 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 SUSCRIPCION DEL CONTRATO

a) Copia de DNI del Representante Legal.
b) Copia de la vigencia del poder del representante legal de la empresa no mayor a sesenta (60) días de antigüedad.
c) Copia del Testimonio 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 (Registro Único de Contribuyente), o registro equivalente para no domiciliados, de ser el caso. Debiendo incluir la fecha de inicio de actividades y los rubros en los que el proveedor brinda sus productos o servicios.
e) Declaración jurada consignando dirección de la oficina o local principal para efectos de notificación u otros fines.
f) Contrato de consorcio con firmas legalizadas de los consorciados, de ser el caso. Acompañando vigencias de poder de ser Personas Jurídicas alguno de los consorciados.
g) Número de cuenta o Código de Cuenta Interbancario (CCI), de corresponder.
h) Garantía de Fiel cumplimiento.
i) Garantía Técnica de las licencias,
j) Otra documentación que sea necesaria para el cumplimiento de la contratación.

7. PLAZO PARA LA SUSCRIPCION DEL CONTRATO

Una vez consentida la buena pro, el postor ganador de la buena Pro deberá presentar toda la documentación requerida para la suscripción del contrato en el plazo de 3 días hábiles. La citada documentación deberá ser presentada en Av. República de Panamá 3531, Piso 9 - San Isidro.

8. PLAZO PARA EL PAGO

La Entidad se compromete a efectuar el pago al contratista en un plazo máximo de 15 días calendario, de otorgada la conformidad de recepción de la prestación.

9. FORMA DE PAGO

AGROBANCO pagará al contratista luego de la adquisición del bien correspondiente. Para hacer efectivo el pago, **EL CONTRATISTA** deberá presentar ante la siguiente documentación:

1. Factura por el servicio contratado
2. Guía de remisión / Certificado de activación
3. Copia del contrato

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:

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

Donde

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

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

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

CAPÍTULO III

ESPECIFICACIONES TECNICAS

"ADQUISICIÓN DE LICENCIAS ANTISPAM Y ANTIVIRUS"

I. OBJETO

AGROBANCO, requiere adquirir 1000 licencias Antispam para el control y protección de buzones de correo electrónicos activos de la organización y 1700 licencias de Antivirus para protección de todo el parque tecnológico de equipos de cómputo entre laptops y equipos servidores que así lo requieran, de acuerdo con las especificaciones técnicas que se detallan en el presente documento.

II. FINALIDAD PUBLICA

La adquisición tiene como finalidad de adquirir y ampliar la protección de todo el parque tecnológico del banco, entre laptops y servidores mediante una herramienta antivirus, así como la protección de todo el tráfico de datos de correo a través de una herramienta antispam.

III. REQUISITOS QUE DEBERA CUMPLIR EL POSTOR

3.1. El POSTOR, deberá estar inscrito en el Registro Nacional de Proveedores del Organismo Supervisor de las contrataciones del Estado.
3.2. El POSTOR, no deberá estar inhabilitado para contratar con el estado peruano.
3.3. El POSTOR, debe garantizar que los bienes ofertados son nuevos, sin uso.
3.4. El PROVEEDOR deberá demostrar por lo menos 5 años (o más) de estar constituido en el mercado local
3.5. El POSTOR deberá ser partner de la marca ofertada, adjuntando una carta de fabricante haciendo referencia al proceso.
3.6. Con la finalidad de garantizar una adecuada implementación del proyecto, el POSTOR, deberá proponer personal calificado, el mismo que deberá cumplir con los requisitos que se indican, según el tipo y ámbito de su competencia.

3.6.1. Un (01) jefe de proyecto

Estará a cargo de la supervisión de toda la solución ofertada. Será el único que coordine con el representante de la División de Infraestructura, Producción y Soporte, la implementación de toda la solución ofertada.

Requisitos:

Título profesional en Ingeniería de Sistemas o Ingeniería de Sistemas e Informática, Ingeniería de Telecomunicaciones o Ingeniería Industrial o Ingeniería de Seguridad y Auditoría Informática o Ingeniería Electrónica o Ingeniería Informática o carreras afines a las tecnologías de la Información; deberá estar colegiado y habilitado al momento de la presentación de la propuesta. Experiencia mínima de tres (03) años como jefe de proyectos de soluciones de seguridad informática. Certificado de Project Management Profesional (PMP) Vigente ó Curso de Gerencia de Proyecto con mínimo de 240 horas de instrucción (Horas Cronológicas); Certificado en ITIL, mínimo v3.

3.6.2. Un (01) especialista para la solución Antivirus. Será encargado de la configuración, despliegue y resolución de problemas en la puesta en marcha de la solución presentada. Requisitos: - Mínimo bachiller ó profesional en Ingeniería de Sistemas e Informática o Ingeniería de Telecomunicaciones o Ingeniería de Electrónica o Ingeniería de Seguridad y Auditoría Informática o Técnico en seguridad informática o Técnico en Redes y Comunicaciones de Datos, o afines a las Tecnologías de la Información. Experiencia no menor de dos (02) en la implementación, soporte técnico y mantenimiento de soluciones de protección de endpoint y servidores. Deben contar con Certificación vigente en el producto ofertado.

3.6.3. Un (01) especialista para la solución AntiSpam, será encargados de la configuración, despliegue y resolución de problemas en la puesta en marcha de la solución presentada. Requisitos: - Mínimo bachiller ó profesional en Ingeniería de Sistemas e Informática, Ingeniería de Telecomunicaciones, Ingeniería de Electrónica, Ingeniería de Seguridad y Auditoría Informática, Técnico en seguridad informática, Técnico en Redes y Comunicaciones de Datos, o afines. Experiencia no menor de dos (02) en la implementación, soporte técnico y mantenimiento de soluciones de protección de correo electrónico. Deben contar con Certificación vigente en el producto ofertado

IV. REQUERIMIENTOS TECNICOS MINIMOS DE LOS BIENES SOLICITADOS

- **DESCRIPCIÓN Y CANTIDAD DE LOS BIENES Y SERVICIOS**

ÍTEM	DESCRIPCIÓN	CANTIDAD	VIGENCIA
1	Licencias Antivirus	1700	1 año
2	Licencias Antispam	1000	1 año

- **CARACTERÍSTICAS TÉCNICAS DEL BIEN**

A continuación, se describirán las etapas correspondientes a esta adquisición:

IV.1. ETAPA 1: PLANIFICACION, ENTREGA Y SUMINISTRO DE EQUIPOS

IV.1.1. Capacidades requeridas
Antivirus.

1. Consola de administración

1.1. Servidor de Administración y Consola Administrativa para Endpoints

- La solución debe disponer de una consola web (https), MMC y Nube para una gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión unificada de la seguridad tanto en modalidad On-Premise como en la Nube.
- Compatibilidad con Windows Failover clustering u otra solución de alta disponibilidad en el caso de consola On-Premise.
- Capacidad de eliminar remotamente cualquier solución de seguridad (propia o de terceros) que esté presente en las estaciones y servidores.

- Capacidad de instalar remotamente la solución en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
- Capacidad de gestionar estaciones de trabajo y servidores (tanto Windows como Linux y Mac) protegidos por la solución;
- Capacidad de gestionar smartphones y tablets (tanto Android y iOS) protegidos por la solución.
- Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
- Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;
- Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
- Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección;
- Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antimalware instalado. En caso de no tenerlo, debe instalar el antimalware automáticamente;
- Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antimalware instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;
- Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;
- Capacidad de importar la estructura de Active Directory para encontrar máquinas;
- Debe permitir bloquear que el usuario cambie las configuraciones de la solución instalada en las estaciones y servidores;
- Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
  - Cambio de gateway;
  - Cambio de subnet DNS;
  - Cambio de dominio;
  - Cambio de servidor DHCP;
  - Cambio de servidor DNS;
  - Cambio de servidor WINS;
  - Aparición de nueva subnet;
- Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet;
- Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;
- La solución debe tener la capacidad de manejar jerarquía de consolas con bases de datos independientes y debe ser multinivel, esto es tener la consola principal (maestra) y otras secundarias (esclavas).
- Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de endpoints;

- Capacidad de herencia de políticas en la estructura jerárquica de servidores administrativos;
- Capacidad de elegir cualquier computadora cliente como repositorio de actualización y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;
- Capacidad de hacer de este repositorio de actualización un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.
- Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
- Capacidad de generar traps SNMP para monitoreo de eventos;
- Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;
- Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (Crystal Reports, por ejemplo).
- Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor);
- Capacidad de realizar inventario de hardware de todas las máquinas clientes;
- Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;
- Capacidad de diferenciar máquinas virtuales de máquinas físicas;
- La solución debe ser capaz de integrarse con soluciones SIEM.
- La solución debe poder enviar notificaciones por correo electrónico.
- La solución debe tener diferentes funciones de administrador que tengan una única interfaz / tablero durante el inicio de sesión y controladas por privilegios y derechos en función de sus roles (Administrador, Revisor, Investigador, etc.).
- La solución debe responder rápidamente en caso de una epidemia de virus, activando una política alternativa preconfigurada desde la consola de administración, donde cualquier configuración del agente de protección pueda ser modificada (desde reglas de firewall, hasta control de aplicativos, dispositivos y acceso a web).
- La solución debe contar con doble factor de autenticación.
- La solución debe admitir el inicio de sesión único (SSO) mediante NTLM y Kerberos.
- La solución debe distribuir automáticamente los equipos a grupos de administración (si aparecen nuevos equipos en la red). Debe brindar la capacidad de establecer las reglas de transferencia o movimiento según la dirección IP, el tipo de sistema operativo y la ubicación en las unidades organizativas de Active Directory.
- La solución debe proporcionar la administración centralizada de los almacenamientos de respaldo y cuarentena en todos los recursos de red donde esté instalado el agente de protección.
- La solución debe tener la funcionalidad para crear múltiples perfiles dentro de una política de protección con diferentes

configuraciones de protección que puedan estar activas simultáneamente en uno o varios dispositivos según las siguientes reglas de activación:

- Estado del dispositivo
- Etiquetas
- Directorio activo
- Propietarios del dispositivo
- Hardware

- La solución debe tener la capacidad de definir un rango de direcciones IP, con el fin de limitar el tráfico de clientes hacia el servidor de administración en función del tiempo y la velocidad.
- La solución debe permitir al administrador establecer un período de tiempo después del cual un ordenador no conectado al servidor de administración, sus datos relacionados se eliminan automáticamente del servidor.
- La solución debe tener una herramienta para recopilar de forma remota los datos necesarios para la resolución de problemas desde los puntos finales, sin necesidad de acceso físico.
- La solución debe permitir al administrador crear un túnel de conexión entre un dispositivo cliente remoto y el servidor de administración si el puerto utilizado para la conexión al servidor de administración no está disponible en el dispositivo.
- La solución debe tener una funcionalidad integrada para conectarse de forma remota al punto final mediante la tecnología de uso compartido de escritorio de Windows. Además, la solución debe poder mantener la auditoría de las acciones del administrador durante la sesión.
- La solución debe incluir soporte para la implementación basada en nube a través de:
  - Amazon Web Services
  - Microsoft Azure

1.2. Compatibilidad

- La solución propuesta debe ser compatible con la instalación en los siguientes sistemas operativos:
- Windows:
  - Windows Server 2008 R2 Standard with Service Pack 1 and later 64-bit
  - Windows Server 2012 Server Core 64-bit
  - Windows Server 2012 Datacenter 64-bit
  - Windows Server 2012 Essentials 64-bit
  - Windows Server 2012 Foundation 64-bit
  - Windows Server 2012 Standard 64-bit
  - Windows Server 2012 R2 Server Core 64-bit
  - Windows Server 2012 R2 Datacenter 64-bit
  - Windows Server 2012 R2 Essentials 64-bit
  - Windows Server 2012 R2 Foundation 64-bit
  - Windows Server 2012 R2 Standard 64-bit
  - Windows Server 2016 Datacenter (LTSB) 64-bit
  - Windows Server 2016 Standard (LTSB) 64-bit
  - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
  - Windows Server 2019 Standard 64-bit
  - Windows Server 2019 Datacenter 64-bit
  - Windows Server 2019 Core 64-bit
  - Windows Server 2022 Standard 64-bit

- Windows Server 2022 Datacenter 64-bit
- Windows Server 2022 Core 64-bit
- Windows Storage Server 2012 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2019 64-bit

Linux:

- Debian GNU/Linux 10.x (Buster) 64-bit
- Debian GNU/Linux 11.x (Bullseye) 64-bit
- Debian GNU/Linux 12 (Bookworm) 64-bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit
- CentOS 7.x 64-bit
- CentOS Stream 9 64-bit
- Red Hat Enterprise Linux Server 7.x 64-bit
- Red Hat Enterprise Linux Server 8.x 64-bit
- Red Hat Enterprise Linux Server 9.x 64-bit
- SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
- SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit
- Astra Linux Common Edition (operational update 2.12) 64-bit
- ALT SP Server 10 64-bit
- ALT Server 10 64-bit
- ALT Server 9.2 64-bit
- ALT 8 SP Server (LKNV.11100-01) 64-bit
- ALT 8 SP Server (LKNV.11100-02) 64-bit
- ALT 8 SP Server (LKNV.11100-03) 64-bit
- Oracle Linux 7 64-bit
- Oracle Linux 8 64-bit
- Oracle Linux 9 64-bit
- RED OS 7.3 Server 64-bit
- RED OS 7.3 Certified Edition 64-bit
- ROSA COBALT 7.9 64-bit

- La solución propuesta debe soportar los siguientes servidores de bases de datos:

  Windows:

  - Microsoft SQL Server 2012 Express 64-bit
  - Microsoft SQL Server 2014 Express 64-bit
  - Microsoft SQL Server 2016 Express 64-bit
  - Microsoft SQL Server 2017 Express 64-bit
  - Microsoft SQL Server 2019 Express 64-bit
  - Microsoft SQL Server 2014 (all editions) 64-bit
  - Microsoft SQL Server 2016 (all editions) 64-bit
  - Microsoft SQL Server 2017 (all editions) on Windows 64-bit
  - Microsoft SQL Server 2017 (all editions) on Linux 64-bit

- Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions)
- Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions)
- Microsoft Azure SQL Database
- All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms
- MySQL 5.7 Community 32-bit/64-bit
- MySQL Standard Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit
- MySQL Enterprise Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit
- MariaDB 10.1 (build 10.1.30 and later) 32-bit/64-bit
- MariaDB 10.3 (build 10.3.22 and later) 32-bit/64-bit
- MariaDB 10.4 (build 10.4.26 and later) 32-bit/64-bit
- MariaDB 10.5 (build 10.5.17 and later) 32-bit/64-bit
- MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine
- MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine
- PostgreSQL 13.x 64-bit
- PostgreSQL 14.x 64-bit
- Postgres Pro 13.x (all editions)
- Postgres Pro 14.x (all editions)

Linux:
- MySQL 5.7 Community 32-bit/64-bit
- MySQL 8.0 32-bit/64-bit
- MariaDB 10.4 (build 10.4.26 and later) 32-bit/64-bit
- MariaDB 10.5 (build 10.5.17 and later) 32-bit/64-bit
- MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine
- PostgreSQL 13.x 64-bit
- PostgreSQL 14.x 64-bit
- PostgreSQL 15.x 64-bit
- Postgres Pro 13.x 64-bit (all editions)
- Postgres Pro 14.x 64-bit (all editions)
- Postgres Pro 15.x 64-bit (all editions)
- Platform V Pangolin 5.4.0 64-bit

- La solución propuesta debe soportar las siguientes plataformas virtuales:

Windows:
- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Microsoft Hyper-V Server 2022 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x

Linux:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Microsoft Hyper-V Server 2022 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Kernel-based Virtual Machine (all Linux operating systems supported by Administration server)

2. Sistemas windows

2.1. Características:

- La solución debe incluir los siguientes componentes dentro de un único agente de protección:
  - Antimalware de archivos
  - Antimalware web
  - Antimalware de correo electrónico
  - Firewall
  - Protección de ataques de red
  - IPS de host (para estaciones de trabajo)
  - Autoprotección (contra ataques a los servicios/procesos del antimalware)
  - Control de dispositivos externos
  - Control de acceso a sitios web
  - Control de ejecución de aplicativos
  - Control de vulnerabilidades de windows y de los aplicativos instalados.
  - Administración de parches de Windows.
  - Cifrado
- La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.
- La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
- La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.
- La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
- La solución debe ser compatible con la interfaz de escaneo antimalware (AMSI).

- La solución debe contar con protección Anti-Ransonware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas. Esta capacidad Anti-Ransonware debe permitir la definición granular de las carpetas a proteger en los servidores.
- La solución debe incluir un componente dedicado a escanear conexiones cifradas.
- La solución debe poder descifrar y escanear el tráfico de red transmitido a través de conexiones cifradas.
- La solución debe permitir anular y reparar las acciones maliciosas que han sido realizadas por el malware, en el sistema operativo, antes de ser detectado.
- Capacidad de elegir qué módulos se instalarán, tanto en instalación local como en la instalación remota;
- Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
- Las actualizaciones de firmas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
- Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- Capacidad de verificar solamente archivos nuevos y modificados;
- Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
- La solución debe incorporar tecnología de autoprotección del agente de protección:
  - Protección contra la gestión remota no autorizada de un servicio de la aplicación.
  - Protección del acceso a los parámetros de la aplicación mediante el establecimiento de una contraseña.
  - Prevención de la desactivación de la protección por parte de malware, delincuentes o usuarios aficionados.
- La solución debe responder rápidamente en caso de una epidemia de virus, activando una política alternativa preconfigurada desde la consola de administración, donde cualquier configuración del agente de protección pueda ser modificada (desde reglas de firewall, hasta control de aplicativos, dispositivos y acceso a web).
- La solución debe permitir detectar y bloquear acciones que no son típicas de los equipos (estaciones de trabajo) en la red empresarial utilizando un conjunto de reglas (escenarios habituales de actividad maliciosa) para supervisar un comportamiento inusual. Estas reglas deben funcionar en modo aprendizaje por al menos dos semanas y luego bloquear o permitir.

- La solución debe incluir un componente de control capaz de aprender a reconocer el comportamiento típico del usuario en estaciones de trabajo, y luego identificar y bloquear acciones anómalas y potencialmente dañinas realizadas por ese equipo o usuario.
- La solución debe ser capaz de bloquear ataques de red e informar la fuente del ataque.
- La solución debe incluir protección contra ataques que exploten vulnerabilidades en el protocolo ARP para falsificar la dirección MAC.
- Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;
- Debe tener módulo IDS/IPS para protección contra port scans y exploración de vulnerabilidades de software.
- El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
  - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
  - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
- Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
- Capacidad de verificar enlaces introducidos en correos electrónicos contra phishings.
- En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
- Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
- Capacidad de modificar los puertos monitoreadas por los módulos de web y correo electrónico;
- En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
  - Bloquear la amenaza, o;
  - Notificar al usuario, con un mensaje de la amenaza, y permitiendo la descarga del objeto.
- Posibilidad de agregar sitios web en una lista de exclusión, donde no serán verificados por el antimalware de web.
- Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (http://www.antiphishing.org/).
- Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas.
- Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
- La solución debe tener la capacidad de restringir las actividades de las aplicaciones dentro del sistema según el nivel de confianza asignado a la aplicación, y limitar los derechos de las aplicaciones

para acceder a ciertos recursos, incluidos los archivos del sistema y de los usuarios (funcionalidad HIPS).

- La solución debe bloquear la ejecución de aplicaciones prohibidas, que están en listas negras, y bloquear la ejecución de aplicaciones que no están en listas blancas. Por tanto, la autorización y denegación de aplicaciones haciendo uso de listas blancas y listas negras debe realizarse sin recurrir a la supervisión de procesos en el sistema operativo del endpoint.
- La solución debe permitir la ejecución de aplicaciones basadas en sus certificados de firma digital, MD5, SHA256, META Data, File Path y categorías de seguridad predefinidas.
- La solución debe soportar un modo de prueba (para el control de aplicaciones) con generación de informes sobre el lanzamiento de aplicaciones bloqueadas, para facilitar posterior configuración en modo bloqueo.
- Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
  - Discos de almacenamiento locales
  - Almacenamiento extraíble
  - Impresoras
  - CD/DVD
  - Drives de disquete
  - Modems
  - Wi-Fi
  - Adaptadores de red externos
  - Dispositivos MTP
  - Dispositivos Bluetooth
  - Cámaras y escáneres
- Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
- Capacidad de configurar las reglas de control de dispositivos por Hardware ID, modelo y máscara del dispositivo.
- La solución debe proporcionar una función Anti-Bridging para las estaciones de trabajo de Windows a fin de evitar puentes no autorizados a la red interna que eludan las herramientas de protección perimetral. Los administradores deben poder prohibir el establecimiento de conexiones simultáneas por cable, Wi-Fi y módem.
- La solución debe ser capaz de registrar operaciones de archivos (escritura y eliminación) en dispositivos de almacenamiento USB. Esto no debería requerir la instalación de ninguna licencia o componente adicional en el punto final.
- La solución debe tener la capacidad de bloquear la ejecución de cualquier archivo ejecutable desde el dispositivo de almacenamiento USB.
- Capacidad de limitar el acceso a sitios web de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.

- La solución debe tener una categoría de detección específica para bloquear los banners del sitio web.
- La solución debe soportar políticas basadas en el usuario para el control de dispositivos, web y aplicaciones.
- La solución debe realizar un borrado remoto de datos en sistemas operativos Windows (estaciones de trabajo), mediante tareas o comandos enviados desde la consola central y ejecutados por el agente de protección. Debe contar con al menos dos modos de eliminación de datos: inmediata y pospuesta (al activarse alguna condición).
- La solución debe tener las siguientes funciones de borrado remoto de datos:
  - En modo silencioso
  - En discos duros y unidades extraíbles
  - Para todas las cuentas de usuario en la computadora
- La funcionalidad de borrado remoto de datos debe admitir los siguientes métodos de eliminación de datos:
  - Eliminación mediante el uso de los recursos operativos: los archivos se eliminan pero no se envían a la papelera de reciclaje.
  - Eliminación completa, sin recuperación: es prácticamente imposible restaurar los datos después de la eliminación.

2.2. Compatibilidad:

Estaciones de trabajo

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

Servidores

- Windows Small Business Server 2011 Essentials / Standard (64-bit)
- Windows MultiPoint Server 2011 (64-bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later
- Windows Web Server 2008 R2 Service Pack 1 or later
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (including Core Mode)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (including Core Mode)
- Windows Server 2016 Essentials / Standard / Datacenter (including Core Mode)
- Windows Server 2019 Essentials / Standard / Datacenter (including Core Mode)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (including Core Mode)

3. Sistemas Linux

3.1. Características:

- La solución debe incluir los siguientes componentes dentro de un único agente de protección:
  - Antimalware de archivos
  - Antimalware web
  - Gestión del firewall
  - Autoprotección (contra ataques a los servicios/procesos del antimalware)
  - Control de dispositivos externos
  - Control de ejecución de aplicativos
- La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.
- La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
- La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.
- La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
- Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:
  - Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
  - Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
  - Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
  - Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
- En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- Capacidad de verificar objetos usando heurística;
- Control de dispositivos conectados con limitaciones de tiempo y de usuario a través de Samba Active Directory y Microsoft Active Directory en la tarea Control de dispositivos.
- Administración del acceso de los usuarios a los dispositivos instalados o conectados por tipo de dispositivo y buses de conexión.
- Escaneo del tráfico HTTP / HTTPS y FTP entrante del equipo del usuario y la detección de direcciones web maliciosas y suplantación de identidad (phishing).

- Debe permitir controlar la ejecución de aplicaciones por medio de la aplicación de listas blancas y listas negras.
- La solución debe proporcionar escaneo de memoria del kernel para estaciones de trabajo Linux.
- La solución debe tener componentes dedicados para monitorear, detectar y bloquear actividades en servidores y estaciones de trabajo, para proteger contra ataques de cifrado remoto.
- La solución debe incluir la capacidad de configurar y administrar configuraciones de firewall integradas en los sistemas operativos, a través de su consola de administración.
- La solución debe tener la capacidad de priorizar tareas de escaneo personalizadas y a demanda.
- La solución debe ser capaz de bloquear ataques de red e informar la fuente del ataque.
- La solución debe incluir protección contra ataques que exploten vulnerabilidades en el protocolo ARP para falsificar la dirección MAC.
- La solución debe proteger sus archivos en los directorios locales contra el cifrado malicioso remoto. Si la solución considera que las acciones de un equipo remoto constituyen un cifrado malicioso, este dispositivo se agrega a una lista de dispositivos no confiables y pierde el acceso a los directorios de red compartidos.

3.2. Compatibilidad:

- Sistemas de 32 bits:
- CentOS 6.7 and later
- Debian GNU / Linux 11.0 and later
- Debian GNU / Linux 12.0 and later
- Mageia 4
- Red Hat Enterprise Linux 6.7 and later
- ALT 8 SP Workstation.
- ALT 8 SP Server.
- ALT Workstation 10
- ALT SP Workstation release 10

- Sistemas de 64 bits
- AlmaLinux OS 8 and later.
- AlmaLinux OS 9 and later.
- AlterOS 7.5 and later.
- Amazon Linux 2.
- Astra Linux Common Edition 2.12.
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.5).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7).
- Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)
- CentOS 6.7 and later
- CentOS 7.2 and later.
- CentOS Stream 8.
- CentOS Stream 9.
- Debian GNU/Linux 11.0 and later.
- Debian GNU/Linux 12.0 and later.
- EMIAS 1.0 and later.
- EulerOS 2.0 SP5.

- Kylin 10.
- Linux Mint 20.3 and up.
- Linux Mint 21.1 and later.
- openSUSE Leap 15.0 and later.
- Oracle Linux 7.3 and later.
- Oracle Linux 8.0 and later.
- Oracle Linux 9.0 and later.
- Red Hat Enterprise Linux 6.7 and later
- Red Hat Enterprise Linux 7.2 and later.
- Red Hat Enterprise Linux 8.0 and later.
- Red Hat Enterprise Linux 9.0 and later.
- Rocky Linux 8.5 and later.
- Rocky Linux 9.1.
- SberLinux 8.8 (Dykhtau).
- SUSE Linux Enterprise Server 12.5 or later.
- SUSE Linux Enterprise Server 15 or later.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- ALT 8 SP Workstation.
- ALT 8 SP Server.
- ALT Workstation 10
- ALT Server 10.
- ALT SP Workstation release 10.
- ALT SP Server release 10.
- Atlant, Alcyone build, version 2022.02.
- GosLinux 7.17.
- GosLinux 7.2.
- MSVSPHERE 9.2 SERVER.
- MSVSPHERE 9.2 ARM.
- RED OS 7.3.
- ROSA Cobalt 7.9.
- ROSA Chrome 12.
- SynthesisM Client 8.6.
- SynthesisM Server 8.6.

- Sistemas de 64 bits ARM
- Astra Linux Special Edition RUSB.10152-02 (operational update 4.7).
- CentOS Stream 9.
- EulerOS 2.0 SP8.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- ALT Workstation 10.
- ALT Server 10.
- ALT SP Workstation release 10.
- ALT SP Server release 10.
- RED OS 7.3.

4. Estaciones Mac OS X

4.1. Características:

- Debe proporcionar protección residente para archivos (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware,

keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.

- La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
- La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.
- La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
- Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;
- Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
- Capacidad de volver a la base de datos de la vacuna anterior;
- Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
- Capacidad de verificar objetos usando heurística;
- Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto;
- Capacidad de verificar archivos de formato de correo electrónico;
- Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antimalware e iniciar el antimalware por la línea de comando;
- Capacidad de ser instalado, removido y administrado por la misma consola central de gestión;

4.2. Compatibilidad:

- MacOS 12 a 14.
- Herramientas de virtualización MAC OS:
  - Parallels Desktop 16 for Mac Business Edition
  - VMware Fusion 11.5 Professional
  - VMware Fusion 12 Professional

5. Smartphones y tablets

5.1. Características:

- La solución debe poder administrar y monitorear dispositivos móviles desde la misma consola que se usa para administrar computadoras y servidores.
- La solución debe poder escanear archivos abiertos en el dispositivo.
- La solución debe poder escanear programas instalados desde la interfaz del dispositivo.

- La solución debe poder escanear objetos del sistema de archivos en el dispositivo o en tarjetas de extensión de memoria conectadas a pedido del usuario o según un cronograma.
- La solución propuesta debe permitir la protección del sistema de archivos del teléfono inteligente y la interceptación y el escaneo de todos los objetos entrantes transferidos a través de conexiones inalámbricas.
- La solución debe proporcionar el aislamiento confiable de objetos infectados en una ubicación de almacenamiento de cuarentena.
- La solución debe incluir la actualización de bases de datos antivirus utilizadas para buscar programas maliciosos y eliminar objetos peligrosos.
- La solución debe poder escanear dispositivos móviles en busca de malware y otros objetos no deseados a pedido y según un cronograma y tratarlos automáticamente.
- La solución debe tener la capacidad de bloquear sitios maliciosos diseñados para difundir códigos maliciosos y sitios web de phishing diseñados para robar datos confidenciales del usuario y acceder a la información financiera del usuario.
- La solución debe tener la funcionalidad de agregar un sitio web excluido del escaneo a una lista de permitidos.
- La solución debe incluir el filtrado de sitios web por categorías y permitir al administrador restringir el acceso del usuario a categorías específicas (por ejemplo, sitios web relacionados con juegos de azar o categorías de redes sociales).
- La solución debe permitir al administrador obtener información sobre el funcionamiento del antimalware y la protección web en el dispositivo móvil del usuario.
- La solución debe tener la funcionalidad para detectar y notificar al administrador sobre ataques al dispositivo (rooteo).
- La solución debe permitir al administrador tomar una fotografía (Mugshot) desde la cámara frontal del móvil cuando este se encuentre bloqueado.
- La solución debe permitir restablecer el PIN de un dispositivo móvil de forma remota.
- La solución debe proporcionar una funcionalidad antirrobo, de modo que los dispositivos perdidos o desplazados se puedan ubicar, bloquear y borrar de forma remota.
- La solución debe proporcionar la posibilidad de bloquear el lanzamiento de aplicaciones prohibidas en el dispositivo móvil.
- La solución debe poder aplicar configuraciones de seguridad, como restricciones de contraseñas y cifrado, en dispositivos móviles.
- La solución debe tener la capacidad de enviar aplicaciones recomendadas o requeridas por el administrador al teléfono móvil.
- La solución debe tener un control de aplicaciones con los modos de aplicación prohibida o permitida.
- La solución debe incluir la opción de enrolar dispositivos mediante sistemas EMM de terceros:
  - VMware AirWatch 9.3 o posterior
  - MobileIron 10.0 o posterior
  - IBM MaaS360 10.68 o posterior
  - Microsoft Intune 1908 o posterior
  - SOTI MobiControl 14.1.4 (1693) o posterior

- La solución debe permitir la configuración de nombres de puntos de acceso (APN) para conectar un dispositivo móvil a servicios de transferencia de datos en una red móvil.
- La solución debe ofrecer controles para garantizar que todos los dispositivos cumplan con los requisitos de seguridad corporativos. El control de cumplimiento debe basarse en un conjunto de reglas que deben incluir los siguientes componentes:
  - Criterios de verificación del dispositivo
  - Plazo asignado para que el usuario solucione el incumplimiento
  - Acción que se tomará en el dispositivo si el usuario no soluciona el incumplimiento dentro del plazo establecido
  - Capacidad para remediar los dispositivos que no cumplen con las normas
- La solución debe tener la funcionalidad de borrar de forma remota lo siguiente de los dispositivos android: datos en contenedores, cuentas de correo electrónico corporativas, configuraciones para conectarse a la red Wi-Fi corporativa y VPN, Nombre del punto de acceso (APN), Perfil de Android for Work, Contenedor KNOX y Clave de KNOX License Manager.
- La solución debe ser compatible con todos los métodos de implementación que se indican a continuación para el agente móvil:
  - Google Play, Huawei App Gallery y Apple App Store
  - Portal de inscripción móvil KNOX
  - Paquetes de instalación preconfigurados independientes
- Para el caso de dispositivos iOS la solución debe:
  - Brindar protección contra amenazas en línea para dispositivos iOS.
  - Tener la funcionalidad para detectar y notificar al administrador sobre ataques al dispositivo (rooteo, jailbreak).
  - Tener la funcionalidad de borrar de forma remota lo siguiente: todos los perfiles de configuración y de aprovisionamiento, el perfil MDM de iOS y aplicaciones para las que se ha seleccionado la casilla de verificación Eliminar.

5.2. Compatibilidad:

- Apple iOS 10.0 o superior.
- iPad OS 13 o superior.
- Android 5 o superior

6. Cifrado de datos:

6.1. Características:

- La solución debe admitir el cifrado para estaciones de trabajo Windows.
- La solución debe admitir el cifrado en varios niveles:
  - Cifrado de disco completo, incluido el disco del sistema
  - Cifrado de archivos y carpetas
  - Cifrado de medios extraíbles
  - Gestionar el cifrado de BitLocker y MacOS Filevault.
- La solución debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que permita:
  - El cifrado de archivos en unidades de computadora locales.
  - La creación de listas de cifrado de archivos por extensión o grupo de extensiones.

  - La creación de listas de cifrado de carpetas en unidades de computadora locales.
- La solución debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que permita el cifrado de archivos en unidades extraíbles. Esto debe incluir la capacidad de:
  - Especificar una regla de cifrado predeterminada por la cual la aplicación aplica la misma acción a todas las unidades extraíbles.
  - Configurar reglas de cifrado para archivos almacenados en unidades extraíbles individuales.
- La solución propuesta debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que admita varios modos de cifrado de archivos para unidades extraíbles:
  - El cifrado de todos los archivos almacenados en unidades extraíbles
  - El cifrado de archivos nuevos solo cuando se guardan o crean en unidades extraíbles.
- La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita cifrar los archivos en unidades extraíbles en modo portátil. Debe permitir el acceso a archivos cifrados en unidades extraíbles que estén conectadas a equipos sin funcionalidad de cifrado.
- La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita cifrar todos los archivos que aplicaciones específicas puedan crear o modificar, tanto en discos duros como en unidades extraíbles.
- La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita la gestión de reglas de acceso de aplicaciones a archivos cifrados, incluida la definición de una regla de acceso a archivos cifrados para cualquier aplicación. Debe permitir el bloqueo del acceso a archivos cifrados o permitir el acceso a archivos cifrados solo como texto cifrado.
- La solución propuesta debe ofrecer la capacidad de restaurar dispositivos cifrados si un disco duro cifrado o una unidad extraíble está dañado.
- La solución propuesta debe ofrecer la funcionalidad de cifrado de disco completo (FDE) integrado para discos duros y unidades extraíbles. Al igual que con FLE, debe existir la capacidad de especificar una regla de cifrado predeterminada mediante la cual la aplicación aplique la misma acción a todas las unidades extraíbles o de configurar reglas de cifrado para unidades extraíbles individuales.
- La solución propuesta debe ofrecer un módulo de cifrado que se administre de manera centralizada en todas las computadoras, con la capacidad de aplicar políticas de cifrado y modificar o detener las configuraciones de cifrado.
- La solución propuesta debe ofrecer la capacidad de monitorear de manera centralizada el estado del cifrado y generar informes sobre las computadoras o dispositivos cifrados.
- La solución propuesta debe ofrecer un cifrado que sea completamente transparente para los usuarios finales y que no tenga un impacto adverso en el rendimiento y el uso del sistema.
- La solución propuesta debe ofrecer cifrado de disco completo que admita la administración centralizada de usuarios autorizados, incluida la adición, eliminación y restablecimiento de contraseñas.

Solo los usuarios autorizados deben tener permiso para iniciar el disco cifrado.

- La solución propuesta debe tener la capacidad de bloquear el acceso de la aplicación a los datos cifrados si es necesario.
- La solución propuesta debe admitir el cifrado automático de dispositivos de almacenamiento extraíbles y debe poder evitar que los datos se copien a medios no cifrados.
- La solución propuesta debe proporcionar una función para crear contenedores protegidos con contraseña que se puedan usar para intercambiar datos con usuarios externos.
- La solución propuesta debe proporcionar una ubicación central para el almacenamiento de claves de cifrado y múltiples opciones de recuperación.
- El servidor de administración o administrador de la solución propuesta debe tener la capacidad de descifrar todos los datos cifrados, independientemente de la ubicación o el usuario.
- La solución propuesta debe admitir tanto los diseños de teclado QWERTY como AZERTY para la autorización previa al arranque.
- La solución propuesta debe admitir la autorización previa al arranque para los siguientes dispositivos: Safe Net eToken 4100, Gemalto IDPrime .NET (511), Rutoken ECP Flash.
- La solución propuesta debe proporcionar la funcionalidad para personalizar la configuración de cifrado de Microsoft BitLocker, lo que incluye:
  - Uso del módulo de plataforma segura y la configuración de contraseñas.
  - Uso de cifrado de hardware para estaciones de trabajo y cifrado de software si el cifrado de hardware no está disponible.
  - Uso de autenticación que requiere la entrada de datos en un entorno previo al arranque, incluso si la plataforma no tiene la capacidad para la entrada previa al arranque (por ejemplo, con teclados de pantalla táctil en tabletas).
- La solución propuesta debe admitir el cifrado en tabletas Microsoft Surface.

7. Gestión de sistemas:

7.1. Características:

- La solución debe tener la capacidad de gestión de sistemas aplicable a plataformas Windows.
- La solución debe incluir funciones para administrar computadoras de forma remota, entre ellas:
  - Instalación remota de software de terceros
  - Generación de informes sobre el software y el hardware existentes
  - Eliminación de software no autorizado
- Capacidad de detectar software de Microsoft y de terceros vulnerables, creando así un informe de software vulnerables.
- Capacidad de corregir las vulnerabilidades de software de cualquier proveedor, haciendo el download centralizado o descentralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.
- Permite la planificación de fecha y hora para el despliegue de parches y actualizaciones, discriminando PCs y Servidores.

- Sincronización con Microsoft Update, para el despliegue centralizado de Parches y actualizaciones Microsoft.
- La solución debe proporcionar la posibilidad de seleccionar qué parches se descargarán o enviarán a los puntos finales, en función de su criticidad.
- La solución debe proporcionar informes completos sobre las vulnerabilidades descubiertas y los parches faltantes, así como sobre los puntos finales y el estado de implementación de los parches.
- La solución debe permitir al administrador aprobar actualizaciones.
- La solución debe poder identificar automáticamente los parches faltantes en los puntos finales individuales e implementar solo los que sean necesarios o falten.
- La solución debe tener la funcionalidad de compatibilidad con el modo de prueba de parches.
- La solución propuesta debe permitir que el administrador configure reglas para la instalación de parches o actualizaciones de Microsoft y de terceros:
  - Iniciar la instalación al reiniciar o apagar la computadora.
  - Instalar los requisitos generales del sistema necesarios.
  - Permitir la instalación de nuevas versiones de aplicaciones durante las actualizaciones.
- Descargar actualizaciones al dispositivo sin instalarlas.
- La solución debe incluir campos dedicados que contengan información sobre "Exploit encontrado para la vulnerabilidad".
- La solución debe incluir campos dedicados que contengan información sobre "Amenaza encontrada para la vulnerabilidad".
- La solución debe poder implementar o enviar archivos EXE, MSI, bat, cmd y MSP de forma remota, y permitir que el administrador defina el parámetro de línea de comandos para la instalación remota.
- Capacidad de gestionar licencias de software de terceros.
- Utilización de Puntos de distribución para el despliegue de parches y actualizaciones en entornos WAN para reducir la utilización de ancho de banda.
- Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, service tag, número de identificación y otros.
- Capacidad de registro de información adicional en los activos de la empresa mediante campos personalizados.

8. EDR

8.1. Características

- La solución debe admitir la detección automatizada de actividad maliciosa mediante tecnologías sandbox.
- La solución sugerida debe complementar la información del veredicto con los artefactos del sistema sobre la detección.
- El agente EDR debe tener integración con la aplicación Endpoint Protection, es decir debe constituir un agente único.
- La solución sugerida debe admitir la generación automática de indicadores de compromiso (IoC) después de que se produzca la detección con la capacidad de aplicar una acción de respuesta.

- La solución debe tener la capacidad de forzar la ejecución de un escaneo de IoC en todos los puntos finales con agentes EDR instalados.
- La solución debe admitir la ejecución de análisis de IoC de acuerdo a una planificación indicada por el administrador o analista.
- La solución debe admitir la importación de IoC de terceros en formato OpenIoC para su uso en el escaneo de los equipos.
- La solución debe admitir el escaneo utilizando un conjunto de IoC generado automáticamente, cargado o externo (de terceros) para detectar amenazas no detectadas anteriormente.
- La solución debe admitir la exportación de IoC generado por la solución a un archivo en formato OpenIoC.
- La solución debe permitir la visibilidad detallada del incidente relacionada con la amenaza detectada en un endpoint.
- La información detallada del incidente debe incluir al menos la siguiente información de la amenaza detectada:
  - 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.
- El gráfico de la cadena de desarrollo de amenazas (kill chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre procesos clave en el dispositivo, conexiones de red, bibliotecas, registro, etc.
- 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:
  - Proceso de spawning
  - Conexiones de red
  - Cambios en el registro
  - Descarga de archivos
  - Dropped de objetos
- La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.
- La solución debe admitir la gestión del agente EDR a través de la interfaz de línea de comandos y por la consola.
- La solución debe tener una función / módulo incorporado para recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
- El agente EDR debe tener un mecanismo de autodefensa para evitar que el agente modifique archivos relacionados con el agente / entradas de componentes del sistema, etc.
- La solución sugerida debe admitir al menos las siguientes acciones de respuesta que un administrador puede realizar cuando se detectan amenazas:
  - Impedir la ejecución de objetos
  - Aislamiento del equipo
  - Eliminar objeto del host o grupo de hosts
  - Terminar un proceso en el dispositivo
  - Poner en cuarentena un objeto

- Ejecutar análisis del sistema
- Ejecución remota de programas/procesos/comandos
- Iniciar escaneo de IoC para un grupo de hosts.

- La solución sugerida debe admitir la integración con el portal de inteligencia de amenazas, que contiene y muestra información sobre la reputación de los archivos y las URL.

8.2. Compatibilidad

- Sistemas listados en el ítem de compatibilidad con sistemas Windows

9. Protección para MS Office 365

9.1. La Solución de Seguridad debe integrarse con Microsoft Office 365 de manera nativa mediante Microsoft Office 365 API sin influir ni requerir cambios en los flujos de tráfico de correo electrónico.

9.2. La solución debe disponer de una consola de gestión que permita la configuración y administración multi-usuario de todas las capacidades ofertadas de manera integral, facilitando la gestión de la seguridad en Microsoft Office 365.

9.3. La solución no debe requerir cambio alguno en los registros MX de correo o en las aplicaciones de Microsoft Office 365 para su funcionamiento.

9.4. La solución debe de validar de Spam, Phishing, Ransomware, BEC, amenazas conocidas y desconocidas en tiempo real para correos electrónicos entrantes, salientes y aquellos que fluyen internamente en la propia instancia de Microsoft Office 365.

9.5. La solucion debe utilizar heurística avanzada, aislamiento de procesos, aprendizaje automático y otras tecnologías de última generación para proteger a las empresas que utilizan Microsoft Exchange Online, Microsoft Teams, Microsoft OneDrive y Microsoft SharePoint Online contra el ransomware, archivos adjuntos maliciosos, spam, phishing, correos electrónicos que comprometen la seguridad de la empresa (BEC) y amenazas desconocidas.

9.6. La solución debe cumplir con el Reglamento General de Protección de Datos (RGDP) y protección de los datos.

9.7. La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware, Anti-BEC & capacidades de filtrado de contenido.

9.8. La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.

9.9. La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.

9.10. La solución debe disponer de capacidades de escaneo bajo demanda sobre buzones de correo pudiendo seleccionar.
- Grupos de usuarios
- Usuarios
- Todos los usuarios"

9.11. La solución debe poder clasificar los correos basura en dos categorías: Spam y correos masivos y poder definir las acciones a tomarse en cada uno de los casos.

9.12. La solución debe contar con capacidades de generar direcciones de lista blanca y negra para cada uno de los módulos de seguridad que propone.

9.13. La solución debe disponer de funciones de validación y autentificación del remitente de manera automática que incluyan:
- DKIM
- DMARK

- SPF"

9.14. La solución debe de disponer de modulo anti malware para la detección oportuna de amenazas conocidas, desconocidas y avanzadas en Microsoft Exchange Online, Microsoft OneDrive, Microsoft SharePoint Online y Microsoft Teams bajo tecnologías de:
- Firmas,
- Análisis heurísticos
- Comportamiento. "

9.15. La solucion debe de disponer una visibilidad unificada de las amenazas detectadas por los sevicios de seguridad base de Microsoft Exchange Online mediante la visualizacion de una cuarentena unica.

9.16. Debe contar con cuadros de mandos, KPIs y reportes de seguimientos de las detecciones realizadas.

9.17. La solución no debe almacenar datos sensibles como usuarios y contraseñas y para esto debe de poder integrase con Microsoft Office 365 mediante OAuth 2.0

9.18. La protección de anti-malware para Microsoft SharePoint Online debe permitir la exclusión y selección de sitios protegidos.

9.19. La protección de anti-malware para Microsoft OneDrive debe permitir la exclusión y selección de usuarios protegidos.

9.20. Debe contar con protección frente a virus, troyanos y otras clases de malware para MS Teams.

9.21. Debe disponer de un módulo de supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por los usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online de la organización relacionadas con datos de tarjetas de crédito.

9.22. La solución debe contar con capacidades de escaneo retrospectivo de amenazas que incluya los buzones de correo y de Ms Office 365 y los repositorios de datos de OneDrive.

9.23. Debe contar con protección basada en firmas mediante aprendizaje automático junto con análisis conductuales y heurísticos avanzados.

9.24. Debe usar una combinación de SPF (marco de directivas de remitente), DKIM (DomainKeys Identified Mail), validación de correo electrónico de DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) y el método de detección de similitudes para detectar y prevenir spoofing y phishing de correos electrónicos, ataques BEC y spam.

9.25. Debe proveer heurística mediante redes neurales de aprendizaje profundo.

9.26. Debe incluir protección contra ataques de inyección de código y mailsploit/spoofing que son posibles debido a los errores de los clientes de correo.

9.27. Debe contar con mecanismo de detección de spam al nivel de la dirección IP.

10. Plataforma de entrenamiento

10.1. La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación.

10.2. La solución propuesta debe dividir el entrenamiento en varios módulos, donde cada uno de los modulo debe estar en una serie de secciones.

10.3. Los módulos propuestos deben incluir teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado.

10.4. La solución propuesta debe permitir descargar un certificado que acredite los logros una vez completadas todas las secciones de un módulo.
10.5. La solución propuesta debe ser 100% en nube
10.6. Los módulos propuestos deben ser de entrenamientos en ciberseguridad agnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicios, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros.

AntiSpam

11. Protección de Servidor de correo electrónico para Windows

Protección Servidores de correo electrónico MS Exchange.

Compatibilidad:

- Microsoft Windows Server 2019 Standard or Datacenter
- Microsoft Windows Server 2016 Standard or Datacenter
- Microsoft Windows Server 2012 R2 Standard or Datacenter
- Microsoft Windows Server 2012 Standard or Datacenter
- Microsoft Windows Small Business Server 2011 SP1 Standard
- Microsoft Windows Server 2008 R2 SP1 Standard, Enterprise or Datacenter

Mail server

- Microsoft Exchange Server 2019 deployed in at least one of the following roles: Mailbox or Edge Transport
- Microsoft Exchange Server 2016 deployed in at least one of the following roles: Mailbox or Edge Transport
- Microsoft Exchange Server 2013 deployed in at least one of the following roles: Mailbox, Edge Transport, or Client Access server (CAS)
- Microsoft Exchange Server 2010 SP3 deployed in at least one of the following roles: Hub Transport, Mailbox, or Edge Transport

Características

- Debe utilizar las tecnologías VSAPI 2.0, 2.5 y 2.6;
- Capacidad de iniciar varias copias del proceso de antivirus;
- Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
- Capacidad de verificar carpetas públicas, correos electrónicos enviados, recibidos y almacenados contra virus, spywares, adwares, gusanos, troyanos y riskwares;
- Capacidad de verificar carpetas públicas y correos electrónicos almacenados de forma agendada, utilizando las últimas vacunas y heurística;

- El antivirus, al encontrar un objeto infectado, debe:
- Desinfectar el objeto, notificando el remitente, destinatario y administradores, o
- Excluir el objeto, sustituyéndolo por una notificación;
- Bloquear el acceso al objeto;
    - Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
    - Caso positivo de desinfección:
    - Recuperar el objeto para uso;
    - Caso negativo de desinfección:
    - Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
- Con anterioridad a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
- Capacidad de enviar notificaciones sobre virus detectados para el administrador, para el destinatario y remitente del mensaje infectado.
- Capacidad de grabar logs de actividad de virus en los eventos del sistema y en los logs internos de la aplicación;
- Capacidad de detectar diseminación en masa de correos infectados, informando al administrador y registrando tales eventos en los logs del sistema y de la aplicación.

12. Protección de Servidor de correo electrónico para Linux

Compatibilidad Sistemas 64-bit:

- Red Hat Enterprise Linux 7.4 Server.
- SUSE Linux Enterprise Server 12 SP3.
- CentOS-6.9.
- CentOS-7.4.
- Ubuntu Server 14.04.5 LTS.
- Ubuntu Server 16.04.4 LTS.
- Debian GNU / Linux 9.4.
- FreeBSD 11.1.

Compatibilidad Sistemas 64-bit:

- ia32-libs for Debian and Ubuntu.
- libgcc.i686, glibc.i686 for Red Hat Enterprise Linux and CentOS.
- libgcc-32bit, glibc-32bit for SUSE.
- lib32 for FreeBSD 64bit.
- compat9x for FreeBSD 11.

MTA:

- Exim-4.86 and later
- Postfix-2.6 and later
- Sendmail-8.14 and later

- Qmail-1.03 and later

Características:

- Capacidad de verificar el tráfico SMTP del servidor contra malware en todos los elementos del correo electrónico: encabezado, cuerpo y adjunto;
- Capacidad de notificar al administrador, al remitente y al destinatario en caso de que un archivo malicioso sea encontrado en el correo electrónico;
- Capacidad de poner en cuarentena objetos maliciosos;
- Capacidad de guardar respaldo de los objetos antes del intento de desinfección;
- Capacidad de hacer barrido en el sistema de archivos del servidor;
- Capacidad de filtrar adjuntos por nombre o tipo de archivo;
- Capacidad de crear grupos de usuarios para aplicar reglas de verificación de correos electrónicos;
- Debe permitir gestión vía consola WEB;
- Debe ser actualizado de manera automática vía internet o por servidores locales, con frecuencia horaria.

13. Seguridad de Correo basada en Mail Gateway Seguro

- Solución de Seguridad para plataforma de correo electrónico en formato Gateway virtual.
- El Virtual Appliance debe ser compatible con en entornos VMWare y Microsoft Hyper-V.
- La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Physhing, Anti-Malware, Anti-Ransomware y de filtrado de contenido.
- La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
- La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.
- La solución debe contemplar la integración de usuarios con openLDAP & Microsoft Active Directory.
- Permite la ejecución de comandos por ejemplo Ping desde interface seleccionada
- Posibilidad de seleccionar tipo de teclado
- Alteración de Zona horaria
- Capacidad de alterar contraseña de acceso a consola Web
- Capacidad de alterar contraseñas de acceso de administrador via Terminal/SSH;
- Verificar comunicación con servidor de actualizaciones
- Capacidad de visualizar logs
- Posibilidad de habilitar acceso en modo soporte para validar configuraciones básicas del appliance virtual.
- Configuración de modulo Anti-Spam vía consola Web.

- Dispone de asistente interactivo para la configuración de la funcionalidad.
- Capacidad de integración con gateway EDGE.
- Posibilidad de agregar dominios locales dentro del alcance.
- Posibilidad de agregar rutas de direccionamiento de dominios
- Posibilidad de agregar redes y direcciones de confianza
- Posibilidad de validación vis SPF
- Debe de verificar si el email del usuario es existente a la hora de recibir un correo.
- Capacidad de verificar logs de mensajes por cantidad y tamaño;
- Capacidad de verificar logs de mensajes enviados por los siguientes.
- Capacidad de monitorizar los recursos del sistema en tiempo real e histórico.
- Capacidad de monitorizar interfaces de envió y recibimiento de mensajes discriminando por tamaño y cantidad de correos y posibilidad de filtro por rangos horarios
- La solución permite la creación de listas Blancas
- La solución permite la creación de listas Negras
- La solución permite la creación de listas de filtrado por contenido
- Capacidad de configurar la solución para la verificación de mensajes.
- Capacidad de rechazar mensajes no verificados
- Posibilidad de excluir mensajes en proceso de verificación.
- La solución permite generar veredictos según el tipo de mensaje:
- En caso de Spam:
  - Ignorar
  - Rechazar
  - Eliminar
  - En caso de posible Spam:
  - Ignorar
  - Rechazar
  - Eliminar
- Capacidad de utilizar tecnologías de procesamiento y reconocimiento de imágenes dentro del alcance del módulo Anti-Spam.
- La solución debe contemplar la validación de objetos del tipo RTF
- La solución debe disponer capacidades de configuración para aumentar el riesgo del mensaje según diccionario de idiomas específicos.
- En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones:
  - Desinfectar
  - Eliminar Anexo
  - Borrar mensaje
  - Rechazar mensaje
  - Ignorar
- La solución permite la personalización de mensajes de texto en el asunto del correo en caso de posible detección de mensajes con amenazas.

- La solución cuenta con funcionalidad para la creación de avisos legales e información de confidencialidad y correos potencialmente inseguros a ser anexos al correo de forma automática.
- La solución permite agregar un aviso legal (Disclamer) de forma automática en mensajes cifrados, de suplantación de identidad, maliciosos o cifrados.
- Capacidad de sincronización con OpenLDAP
- Capacidad de sincronización con directorio activo de Microsoft (MS AD)
- La solución permite agregar remitentes y destinatarios basándose por lo menos en la dirección de correo electrónico, dirección IP y cuenta LDAP.
- Soporte a criptografía TLS
- Permite tomar acción ante TLS rechazado, aceptado o obligatorio.
- Soporte a protocolos SMTP e LMTP
- La solución cuenta con funcionalidad e backup y permite limitar el tamaño máximo del mismo.
- Configuración de notificaciones según limite disponible de espacio en disco.;

IV.1.2. Actividades de Preparación

a) El POSTOR en coordinación con el equipo técnico del BANCO deberán identificar las áreas de mejora.
b) El postor deberá de plantear el método de instalación y despliegue utilizando alguna herramienta que permita realizar esto de forma masiva.
c) Coordinar con el equipo de TI interno sobre la estrategia de puesta en operación y las ventanas de tiempo que van a ser requeridas.

IV.1.3. Planificación:

a) Desarrollo de un calendario detallado que incluya todas las fases del proyecto desde la adquisición hasta la puesta en operación.
b) Kickoff del proyecto, reunión inicial con todo el equipo, tanto de parte del POSTOR, así como del BANCO para sensibilizar las actividades a realizar.
c) Plan del proyecto, socializar y entregar el plan de proyecto para la implementación que contenga al menos los principales planes como la gestión del alcance, tiempo, recursos, calidad, riesgos, comunicación.

IV.1.4. Condiciones de Entrega:

a) Las licencias de la solución antivirus deberán entrar en vigencia al culminar el despliegue en los equipos finales, para lo cual es postor deberá proporcionar licencias temporales hasta el término del despliegue con la finalidad de asegurar la continuidad de la protección para no comprometer la seguridad de los sistemas del banco.
b) Las licencias de la solución Antispam deberán entrar en vigencia al culminar la configuración de la solución evidenciando el correcto control del flujo de tráfico de correo.

IV.2 ETAPA 2: IMPLEMENTACION

Durante esta etapa se tendrá que realizar las siguientes actividades:

IV.2.1. Instalación y Configuración

a) Registrar y activar las licencias en el sistema del fabricante para su distribución.

b) El POSTOR deberá realizar la instalación y configuración de la herramienta Antispam para todos los buzones contratados.
c) El POSTOR deberá realizar la instalación y configuración de la herramienta Antivirus en los equipos del banco, asegurando un mínimo de 300 equipos (incluyendo la desinstalación de la solución antivirus actual instalada), (Servidores y Laptops) en la Oficina principal, de acuerdo con lo establecido en el Plazo de Entrega.
d) Para la red de agencias, el POSTOR deberá asegurar la instalación y configuración de la herramienta Antivirus en un mínimo de 400 equipos (incluyendo la desinstalación de la solución antivirus actual instalada), de acuerdo con lo establecido en el Plazo de Entrega.
e) El POSTOR implementará los mecanismos necesarios para el despliegue de licencias en todos los equipos del BANCO, dado a que los equipos están tanto en Oficina Principal como en todas las oficinas que están en las distintas ubicaciones dentro del territorio peruano.
f) Configurar las opciones básicas de protección y antispam según las políticas definidas.
g) Ajustar configuraciones avanzadas para proteger servidores críticos y asegurar la compatibilidad con aplicaciones existentes
h) Configurar políticas de protección antivirus y antispam, incluyendo niveles de detección y acciones a tomar ante amenazas detectadas.
i) Establecer excepciones para aplicaciones legítimas que podrían ser identificadas erróneamente como amenazas.

IV.2.2. Migración de Políticas y Reglas

a) Migración de las políticas de acceso existentes a la nueva solución como punto de partida.
b) Verificación de que las políticas migradas funcionan correctamente y cumplen con los requisitos de seguridad.

IV.2.3. Pruebas y Validación

a) Verificar que el software antivirus y antispam se instala correctamente y que las funciones básicas operan según lo esperado.
b) Realizar pruebas de detección de malware y spam para asegurar que la solución identifica y maneja adecuadamente las amenazas
c) Evaluar el impacto de la solución en el rendimiento de los equipos y servidores, asegurando que no afecte negativamente las operaciones diarias.
d) Asegurar que las políticas de seguridad están correctamente implementadas y que la solución no introduce nuevas vulnerabilidades

IV.2.4. Conformidad y Puesta en operación:

a) Luego de realizar las pruebas y ser satisfactorias las mismas, el POSTOR deberá presentar el acta de conformidad sobre el alcance del servicio solicitado.
b) La puesta en operación de las soluciones solicitadas, la realizará el personal del POSTOR.

IV.2.5. Capacitación y Transferencia de Conocimiento

a) Formación al equipo de TI y administradores que determine Agrobanco sobre el uso y gestión de las soluciones.
b) Provisión de manuales de usuario, guías de configuración y procedimientos operativos estándar.
c) El POSTOR deberá brindar un servicio de Capacitación de 03 horas para hasta 4 personas quien deberá entregar un syllabus con los temas a tratar, los mismos que deberán ser aprobados por la ENTIDAD mediante un correo electrónico enviado por el Especialista de

Infraestructura y Producción de la ENTIDAD y/o Jefe de Infraestructura, Producción y Soporte.

d) Se deberá entregar certificados de participación, firmados por el personal capacitador.

IV.3 ETAPA 3: OPERACIÓN

Durante esta etapa se podrán ejecutar las siguientes actividades:

IV.3.1. Soporte técnico:

a) El POSTOR debe contar con una Mesa de ayuda como un único punto de contacto para atender cualquier requerimiento y/o incidente y estar en la capacidad de dar soporte y solución a los incidentes que son reportados.

b) Se solicita contar con una bolsa de 80 horas adicionales de soporte local para atender incidentes y requerimientos derivados del proceso de implementación.

c) En el caso que las horas adicionales no se hayan utilizado durante el año, podrán usarse para capacitaciones las mismas que serán acordadas entre el POSTOR y el Jefe de la División de Infraestructura Producción y Soporte.

d) Se debe contar con soporte técnico integral para las soluciones ofertadas (en hardware y software) que incluya actualizaciones de software, reparaciones, reemplazos y otros de hardware que garanticen mantener siempre operativa la solución implementada.

e) El acceso a la mesa de ayuda para la generación de una atención de servicio debe contener como mínimo:
   - Poder realizar un requerimiento mediante llamada local.
   - Mediante el envío de un correo electrónico.
   - Mediante el uso de un formulario web definido por el postor.

f) Todo incidente de orden técnico o funcional es atendido en un primer nivel el POSTOR local y de requerir escalar al fabricante, será a través del POSTOR, el cual realizará los contactos con el fabricante.

g) Dependiendo de la complejidad de la incidencia, la atención en primera instancia podrá ser vía telefónica con el soporte técnico local, si no es posible la solución por este medio, podrá ser vía acceso remoto y en una tercera instancia será la visita de técnicos a las oficinas de Agrobanco.

h) Cuando se presente una situación excepcional que le impida cumplir con el tiempo estipulado para la solución, el POSTOR podrá enviar una Carta y/o correo electrónico a la División de Infraestructura, Producción y Soporte exponiendo los motivos que originaron la situación, con la finalidad de evaluar las justificaciones.

i) Las licencias y el soporte de fabricante deben cubrir reemplazos de equipos y soporte por el periodo de 1 año contados a partir de la firma de conformidad del servicio implementado.

j) Como parte del servicio, el proveedor debe ser capaz de gestionar y responder ante incidentes. Para ello el proveedor debe contar con una solución de tipo SIEM (Security Information Event Management) que le permita detectar, responder y neutralizar las amenazas informáticas que sean detectadas por las soluciones que formarán parte del presente servicio: Antivirus y Antispam, incluyendo la solución de filtro web Barracuda presente en el banco.

IV.3.2. Mantenimiento:

a) El POSTOR realizará 1 mantenimiento de las soluciones adquiridas en coordinación con el BANCO al 6to mes de iniciado el servicio contratado, debiendo detallar las actividades a ejecutar.
b) El POSTOR deberá presentar el rol del mantenimiento con el detalle de las actividades a ejecutar el mismo que deberá ser proporcionado al culminar la fase de implementación.
c) El POSTOR notificará al personal de la división de Infraestructura con 30 días de antelación del inicio del mantenimiento.
d) El personal del POSTOR que realizará el mantenimiento deberá contar con las características del perfil técnico indicadas en el literal III (relacionado al personal).

IV.3.3. Garantía:

a) Los componentes deberán ser nuevos y originales según el número de parte del fabricante. No se aceptarán componentes de mercado secundario o refurbished.
b) Presentar carta del fabricante que se indique que los componentes son nuevos y originales
c) Todo el equipamiento (hardware y software) debe contar con garantía de fábrica y del POSTOR de un (1) año a partir de la conformidad del servicio de la puesta en operación de la solución, emitida por la División de Infraestructura, Producción y Soporte, con alcance de 24 horas del día, los 7 días de la semana, los 365 días del año.
d) Los repuestos, mano de obra y otros que puedan incurran por el servicio brindado, serán sin costo adicional para AGROBANCO.
e) El POSTOR del servicio no podrá alegar inconvenientes con el fabricante para la provisión de los trabajos de asistencia técnica mencionados, debiendo garantizar en toda circunstancia la posibilidad de escalamiento de estos eventos.
f) El POSTOR, deberá gestionar la reposición de los componentes o partes que se requieran para la reparación de los equipos proporcionados en caso estos los requiera.
g) Cuando se tenga la necesidad de cambiar un equipo, este será recogido de la oficina principal de AGROBANCO

IV.3.4. Niveles de Servicio (SLA)

Una vez que el equipamiento se encuentre en operación, se aplicara los siguientes niveles de servicio. La penalidad se aplicará a la factura del periodo vigente del servicio de soporte:

SLA	Penalidad	
	Tiempo	%
Nivel 1 CRITICO (*Indisponibilidad parcial o total del servicio*)		
Tiempo de respuesta: Máximo 1 hora para un contacto remoto (telefónico y/o control remoto)	> 1 hora	15%
Tiempo de solución: Máximo 4 horas	> 4 horas	50%
Nivel 2 ALTO (*Toda incidencia que no represente indisponibilidad del servicio, ni represente una afectación de seguridad crítica a los sistemas del banco.* *Otros incidentes derivados por temas de desempeño y/o configuración de las herramientas adquiridas***)**		
Tiempo de respuesta: Máximo 4 horas	> 4 horas	10%
Tiempo de solución: Máximo 12 horas	> 12 horas	40%
Requerimientos		
Tiempo de atención: Máximo 48 horas	> 48 horas	5%
Mantenimiento Preventivo		
No realizar el mantenimiento preventivo en la fecha comprometida.	Por fecha incumplida	30%

Las penalidades pueden alcanzar un monto máximo equivalente al nueve por ciento (9%) del monto del contrato.

V. LUGAR DE ENTREGA DEL BIEN

El bien deberá ser entregado en la Oficina Principal de AGROBANCO: Av. República de Panamá 3531, piso 5, San Isidro.

VI. PLAZO DE ENTREGA

El plazo de entrega de los bienes objeto de la contratación, tendrá los siguientes plazos:

Etapa 1:
El plazo de entrega de las licencias será de hasta quince (15) días calendario, contado a partir del día siguiente de la firma del contrato.

Entregables:

- Plan del proyecto
- Acta de Kickoff
- Cronograma de actividades que será entregado máximo en 10 días posterior a la firma del contrato.
- Presentación del certificado/licencia de garantía, soporte y derecho a actualizaciones.
- Guías de Remisión de los bienes
- Acta de conformidad de la entrega de licencias.
- Factura por la entrega del bien.

Etapa 2:
El plazo máximo para realizar la implementación de la solución se realizará hasta los sesenta (60) días calendarios contados a partir de la conformidad de la etapa 1.

La activación de las licencias será culminada el periodo de Instalación, configuración y puesta en producción de las soluciones ofertadas.

Entregables

- Acta de instalación de los equipos.
- Matriz de escalamiento.
- Plan de mantenimiento Preventivo.
- Informe técnico final de Instalación, configuración y puesta en operación de la
- solución ofertada que deberá entregar al finalizar la implementación emitido por el POSTOR, entre los que se detallarán:
- Evidencia de activación de las licencias Antispam
- Evidencia de tráfico de correo desde la consola antispam
- Evidencia de activación de las licencias Antivirus (consola y en los equipos instalados)
- Relación de equipos configurados con la licencia antivirus activa
- Acceso administrador a las consolas de gestión
- Acta y Certificados del personal participante de la capacitación
- Acta de conformidad de la implementación.
- Factura por la implementación.

Etapa 3:

El plazo de esta etapa de operación es de 12 meses que dura el contrato.

Soporte

- El soporte técnico iniciara después de firmada el acta de implementación (puesta en operación de todos los equipos) y se realizara por un periodo de 12 meses.

Mantenimiento

- Se realizarán 1 mantenimiento preventivo durante el tiempo del servicio contratado. Contados a partir de la firmada del acta de implementación (puesta en operación de las soluciones)

Entregables

- El POSTOR deberá elaborar y entregar informes mensuales sobre el uso, comportamiento y estadísticas de seguridad de las herramientas implementadas que serán remitidos a Agrobanco vía correo electrónico dentro de los 10 primeros días de cada mes, pudiendo también ser solicitado a demanda de acuerdo sea requerido por AGROBANCO.
- Informe del mantenimiento programado adjuntando evidencias de las actividades realizadas que debe ser entregado dentro de los 5 días posterior al término del trabajo.
- Factura por el soporte técnico.

Toda la documentación técnica proporcionada por el POSTOR deberá entregarse en forma electrónica a los siguientes correos: jrodriguezr@agrobanco.com.pe y rcoronado@agrobanco.com.pe.

VII. FORMA DE PAGO

- PRIMER PAGO DEL 60%, posterior a la firma del acta de entrega de Licencias.

- SEGUNDO PAGO DEL 28%, Posterior a la firma del Acta de implementación de las soluciones por parte de Agrobanco.

- TERCER PAGO DEL 12%, por el Soporte Técnico, para atender los incidentes y requerimientos, esto se realizará de forma cuatrimestral a razón de 4% al mes 4, 4% al mes 8 y 4% al mes 12.

VIII. CONFORMIDAD DEL BIEN

Para efecto del trámite de pago, la Gerencia de Transformación Digital e Innovación deberá otorgar la conformidad del bien dentro de un plazo de 15 días hábiles posterior a la firma del acta de implementación y de haber recepcionado la factura o comprobante de pago correspondiente.

CAPÍTULO IV

CRITERIOS DE EVALUACIÓN

EVALUACIÓN TÉCNICA
(Puntaje Máximo: 100 Puntos)

A fin de permitir la selección de la mejor oferta en relación con la necesidad que se requiere contratar, se consigna los siguientes factores de evaluación:

CRITERIOS DE EVALUACION	PUNTAJE
A. Experiencia del postor	80.00
B. Mejoras previstas en las bases	20.00
PUNTAJE TOTAL	**100.00**

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 contrato. 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°13. 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 cuatro (4) veces el valor referencial.

Tal experiencia se acreditará mediante (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente (el postor podrá presentar entre otros: voucher de depósito, nota de abono, 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 la venta y/o soporte y/o actualización de licencias Antispam o Antivirus, o afines directamente relacionados al objeto de la presente convocatoria.**

La asignación de puntaje será de acuerdo al siguiente criterio:

CRITERIO EXPERIENCIA DEL POSTOR: MONTO FACTURADO ACUMULADO	**Puntos**
Monto acumulado igual o mayor a 4 veces el valor referencial	80.00
Monto acumulado igual o mayor a 3 veces el valor referencial y menor a 4 veces el valor referencial	70.00
Monto acumulado igual o mayor a 1 vez el valor referencial y menor a 3 veces el valor referencial	60.00
Monto menor a 1 vez el valor referencial	0.00

B. MEJORAS PREVISTAS EN LAS BASES **Máximo 20.00 puntos**

Se calificará la mejora en el plazo de la garantía solicitada.

El postor ofrece mejora en la garantía….....20.00 puntos
El postor No ofrece mejora en la garantía.....00.00 puntos

A efecto de obtener el puntaje en el presente factor, el postor deberá presentar la Declaración Jurada de Garantía - **Anexo Nº07.**

PARA ACCEDER A LA ETAPA DE EVALUACIÓN ECONÓMICA, EL POSTOR DEBERÁ OBTENER UN PUNTAJE TÉCNICO MÍNIMO DE OCHENTA (80.00) PUNTOS.

Se aceptarán ofertas 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 Pro se utilizará la siguiente ponderación:

Oferta Técnica : 0.60
Oferta Económica: 0.40

CAPÍTULO V

PROFORMA DE CONTRATO

Conste por el presente documento, el contrato que celebran, (de manera conjunta se les denominará las "PARTES"), de una parte, el BANCO AGROPECUARIO, con RUC Nº 20504565794, con domicilio en Av. República de Panamá Nº 3531 Oficina 901, Distrito de San Isidro, Provincia y Departamento de Lima, debidamente representado por……., identificado con DNI Nº……., y……, identificado con DNI Nº……., según poderes inscritos en la Partida Electrónica Nº 11382875 del Registro de Personas Jurídicas de Lima, a quienes en adelante se le denominará "AGROBANCO" y de otra parte……, con RUC Nº ……., con domicilio legal en ……., Lima debidamente representado por ……. con DNI N° ……, según poder inscrito en la Partida N° ……, del Registro de Personas Jurídicas de Lima, a quien en adelante se le denominará "EL CONTRATISTA" en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha ……, el Comité adjudicó la Buena Pro de la **ADQUISICIÓN NIVEL II Nº0024-2024-AGROBANCO "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS,** cuyos detalles e importes totales, constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

Por el presente instrumento **EL CONTRATISTA** se compromete a prestar a favor de **AGROBANCO** la **ADQUISICIÓN NIVEL II Nº0024-2024-AGROBANCO "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS,** con arreglo a las Bases, Términos de Referencia y Oferta Técnica y Económica presentada, documentos que forman parte del presente contrato.

CLÁUSULA CUARTA: MONTO CONTRACTUAL

El monto total del servicio materia del presente contrato asciende a S/xxxx (xxxxxx con 00/100 SOLES) a todo costo, incluido IGV.

Este monto comprende los costos del bien, transporte hasta el punto de entrega, seguros e impuestos, así como todo aquello que sea necesario para la correcta ejecución de la prestación materia del presente contrato.

CLÁUSULA CUARTA: FORMA DE PAGO

AGROBANCO se obliga a pagar la contraprestación a EL CONTRATISTA, previa presentación de la factura correspondiente. Para hacer efectivo el pago, el responsable de dar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los quince (10) días hábiles de ser estos recibidos, a fin de permitir que el pago se realice dentro de los quince (15) días calendarios siguientes.

CLÁUSULA QUINTA: INICIO Y CULMINACIÓN DE LA PRESTACIÓN

El plazo de ejecución del servicio será conforme lo establecido en el numeral **VI. Plazo de Entrega** de las especificaciones técnicas. Este plazo será contabilizado a partir del día siguiente de la suscripción del contrato.

Una vez que el equipamiento se encuentre en operación, se aplicara los siguientes niveles de servicio. La penalidad se aplicará a la factura del periodo vigente del servicio de soporte

SLA	Penalidad	
	Tiempo	%
Nivel 1 CRITICO (*Indisponibilidad parcial o total del servicio*)		
Tiempo de respuesta: Máximo 1 hora para un contacto remoto (telefónico y/o control remoto)	> 1 hora	15%
Tiempo de solución: Máximo 4 horas	> 4 horas	50%
Nivel 2 ALTO (*Toda incidencia que no represente indisponibilidad del servicio, ni represente una afectación de seguridad crítica a los sistemas del banco.* *Otros incidentes derivados por temas de desempeño y/o configuración de las herramientas adquiridas***)**		
Tiempo de respuesta: Máximo 4 horas	> 4 horas	10%
Tiempo de solución: Máximo 12 horas	> 12 horas	40%
Requerimientos		
Tiempo de atención: Máximo 48 horas	> 48 horas	5%
Mantenimiento Preventivo		
No realizar el mantenimiento preventivo en la fecha comprometida.	Por fecha incumplida	30%

Las penalidades pueden alcanzar un monto máximo equivalente al nueve por ciento (9%) del monto del contrato.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las Bases integradas, la oferta ganadora y los documentos derivados del proceso de selección que establezcan obligaciones para las partes.

CLÁUSULA SEPTIMA: CONFORMIDAD DE LA PRESTACION

La conformidad de la prestación estará a cargo de la Gerencia de Gestión y Desarrollo del Talento Humano y la División de Desarrollo del Talento Humano.

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

Este procedimiento no será aplicable cuando el servicio manifiestamente no cumpla con las características y condiciones ofrecidas, en cuyo caso AGROBANCO no efectuará la recepción, debiendo considerarse como no ejecutada la prestación, aplicándose las penalidades que correspondan.

CLÁUSULA OCTAVA: PREVENCION DE LAVADO DE ACTIVOS Y DE FINANCIAMIENTO DEL TERRORISMO

El CONTRATISTA declara que la conformación de su patrimonio y que sus ingresos no provienen de actividades de Lavado de Activos y del Financiamiento del Terrorismo y en general de cualquier actividad ilícita; de igual manera declara que el destino de los ingresos que genere el presente contrato no será utilizado para actividades delictivas.
EL CONTRATISTA mantendrá el deber de reserva en forma indeterminada de la información relacionada con el Sistema de Prevención de Lavado de Activos y del Financiamiento del Terrorismo, sobre la que haya tomado conocimiento como consecuencia del servicio prestado, su incumplimiento será considerado como causal de resolución del presente contrato, sin perjuicio de las acciones civiles y penales que correspondan.
Asimismo, en caso de ser Sujeto Obligado de acuerdo con lo dispuesto por la Ley Nº 27693 y sus normas modificatorias y complementarias, se compromete a entregar a **AGROBANCO**, la documentación e información que ésta requiera, con la finalidad de sustentar que **CONTRATISTA** viene cumpliendo con las normas de Prevención de Lavado de Activos y del Financiamiento del Terrorismo."

CLÁUSULA NOVENA: SEGURIDAD DE INFORMACION O PROCESAMIENTO DE DATOS (de corresponder)

Las partes acuerdan que la totalidad de la información obtenida por su contraparte con motivo de la ejecución del presente contrato es de exclusiva propiedad de ambas partes, obligándose las mismas a utilizarlas sólo para los fines del presente contrato.

La aplicación de la presente cláusula está condicionada a que el/los servicio(s) y/o producto(s) contratados se encuentren vinculados al tratamiento de datos personales, de lo contrario sus estipulaciones se entenderán como no puestas, total o parcialmente.

LAS PARTES se obligan a proteger los datos personales entregados por su contraparte, los que pudiera tener acceso en ejecución del presente contrato y/o los que se generen como consecuencia de este (en lo sucesivo, "Los Datos") implementando las medidas de seguridad y confidencialidad necesarias para su resguardo y acordes con el tratamiento que vaya a efectuarse; evitando su alteración, pérdida, tratamiento y/o acceso no autorizado. Asimismo, LAS PARTES se obligan a cumplir todas las disposiciones que le correspondan, de conformidad con la Ley N° 29733 – Ley de Protección de Datos Personales; su reglamento aprobado mediante Decreto Supremo N° 003-2013- JUS; las demás disposiciones complementarias, modificatorias y/o aclaratorias presentes y/o futuras; así como las que establezca la Autoridad Nacional de Protección de Datos Personales.

Es obligación de LAS PARTES tratar "Los Datos" a razón de lo estrictamente establecido en el presente contrato, encontrándose imposibilitada de utilizarlos para una finalidad distinta o en beneficio propio o de terceros y/o transferirlos sin que medie autorización previa, expresa y escrita por parte de su contraparte, salvo que ello resulte necesario para la ejecución del presente contrato, lo cual deberá ser puesto en conocimiento de su contraparte previamente y por escrito. En este escenario, LAS PARTES garantizan a su contraparte que el o los receptores de "Los Datos" a los que recurrirá para el cumplimiento de sus obligaciones mantienen niveles de protección y seguridad, según las condiciones previstas en el presente contrato; siendo responsable a su vez de asegurar que el o los receptores que participen en el tratamiento de "Los Datos" cumplan con las disposiciones previstas en la presente cláusula.

LAS PARTES garantizan a su contraparte que "Los Datos" serán tratados únicamente por aquellos empleados o terceros cuya intervención resulte imprescindible para la ejecución del presente contrato; asegurando a su vez que pondrá en conocimiento de

estos las medidas de seguridad que han de observar; y, el deber de confidencialidad que han de tener respecto de "Los Datos", inclusive finalizada la prestación de servicios.

De realizarse flujo transfronterizo de datos personales, LAS PARTES deberán implementar niveles suficientes de protección para los datos personales que se vayan a tratar, de acuerdo con lo previsto en la legislación peruana o por los estándares internacionales en la materia. Asimismo, LAS PARTES deberán establecer cláusulas contractuales que establezcan que el receptor de la información tiene las mismas obligaciones que LAS PARTES en relación a los Datos Personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales

Asimismo, LAS PARTES se obligan a dar a conocer los cambios en sus políticas de privacidad o en las condiciones del servicio que presta. LAS PARTES permitirán y contribuirán a la realización de auditorías e inspecciones realizadas por su contraparte y/o terceros designados por este, con el objeto de verificar el cumplimiento de las obligaciones que le resulten aplicables en su condición de encargado y/o responsable de tratamiento.

Concluida la relación contractual o a simple solicitud de su contraparte, **LAS PARTES** se obliga a eliminar "Los Datos" de todos sus sistemas y/o archivos en cualquier formato, debiendo para ello entregar una declaración jurada que sustente el cumplimiento de esta obligación.

En caso cualquiera **LAS PARTES** sea quien suministre a su contraparte datos personales, aquella declara que los mismos han sido recabados, adquiridos y/o actualizados, según corresponda, con arreglo al marco normativo sobre protección de datos personales, lo cual involucra la licitud de su origen y el respeto de todos los principios rectores del derecho de protección de datos personales.

LAS PARTES serán responsables por los reclamos, denuncias, procesos judiciales, procedimientos administrativos y/o cualquier otro iniciado en contra de la otra parte**;** así como por los daños y perjuicios derivados del incumplimiento de las obligaciones establecidas en la presente cláusula, en tanto le resulten imputables. En ese sentido, **LAS PARTES** se harán cargo de las costas, costos, gastos, multas, indemnizaciones, así como cualquier otro gasto en que se incurra.

LAS PARTES se obligan a no realizar ninguna subcontratación de los servicios objeto del presente contrato, que implique la comunicación a terceros distintos a las partes, de los datos personales a los que tiene acceso como consecuencia de la ejecución del presente contrato. En caso se requiera subcontratar con terceros, parte de los servicios, se deberá contar con autorización por escrito de su contraparte y el subcontratista asumirá idénticas obligaciones a las establecidas para el prestador del servicio en el presente contrato respecto de los datos personales de **LA COMPAÑÍA** o **EL BANCO**.

LAS PARTES declaran conocer la Política de Privacidad que tiene su contraparte, manifestando su compromiso a adherirse a los lineamientos incluidos en la misma, así como lograr la adhesión correspondiente por parte de todos sus empleados y de las personas que actúan a su nombre.

CLÁUSULA DECIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DECIMO PRIMERA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad de recepción de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, hasta en el plazo de 1

año.

CLÁUSULA DÉCIMO SEGUNDA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplicará al contratista una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato La penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

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

Donde

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

Tanto el monto como el plazo se refieren, según corresponda, al contrato o ítem que debió ejecutarse o, en caso que éstos involucrarán obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

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

Esta penalidad será deducida de los pagos a cuenta, del pago final o en la liquidación final; o si fuese necesario se cobrará del monto resultante de la ejecución de las garantías de Fiel Cumplimiento o por el monto diferencial de la oferta (de ser el caso).
La justificación por el retraso se sujeta a lo dispuesto por el Código Civil y demás normas concordantes.

CLÁUSULA DÉCIMO CUARTA: RESOLUCIÓN DEL CONTRATO

Constituirán causales de resolución, previa notificación, del presente contrato las siguientes:

1. El acuerdo mutuo de ambas partes.
2. El incumplimiento parcial, tardío o defectuoso de cualquiera de las obligaciones a cargo de EL CONTRATISTA contenidas en el presente contrato.
3. Por fuerza mayor o caso fortuito calificados de conformidad con lo previsto en la ley.
4. Unilateralmente por incumplimiento reiterado de cualquiera de las partes de las obligaciones a su cargo (sin perjuicio de las acciones a que haya lugar en virtud de dicho incumplimiento)
5. Por terminación unilateral anticipada previa comunicación escrita remitida a la otra parte con una antelación no menor de treinta (30) días, sin que por esto se entienda que hay lugar al cobro de indemnización alguna a favor de la otra parte

CLÁUSULA DÉCIMO CUARTA: RESPONSABILIDAD DEL CONTRATISTA

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

CLÁUSULA DÉCIMO QUINTA:MODELO DE PREVENCIÓN DE DELITOS (ANTICORRUPCIÓN)

15.1 EL PROVEEDOR / CONTRAPARTE declara de manera expresa, incondicional e irrevocable, y bajo responsabilidad, que no ha infringido ni ha vulnerado, y que no infringirá ni vulnerará alguna cualesquiera de las normas que regulan la

responsabilidad administrativa de las personas jurídicas, en el marco de lo dispuesto por la Ley N° 30424 y normas modificatorias, sustitutorias y/o complementarias, y lo señalado en el Decreto Legislativo N° 1106, Decreto Legislativo de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado y normas modificatorias, sustitutorias y/o complementarias. De igual manera, **EL PROVEEDOR / CONTRAPARTE** declara de manera expresa, incondicional e irrevocable, y bajo responsabilidad que no ha cometido ni cometerá, los delitos tipificados en los Artículos 384, 397, 397-A, 398 y 400 del Código Penal Peruano vigente ni otros cualesquiera delitos análogos que afecten la relación contractual entre las partes que suscriben el presente Contrato y generen un perjuicio a la reputación de AGROBANCO, al leal saber y entender de este último.

15.2 Teniendo en cuenta lo indicado, **EL PROVEEDOR / CONTRAPARTE**, declara conocer y se compromete a cumplir todas y cada una de las siguientes políticas de prevención de Corrupción; asimismo, se compromete a tomar todas y cada una de las medidas necesarias, con el objeto de que sus subcontratistas, agentes y/o cualquier otro tercero que esté sujeto a su control, cumplan, en su totalidad, con las políticas de prevención de AGROBANCO, las mismas que se detallan a continuación:

a. **EL PROVEEDOR / CONTRAPARTE** se compromete a mantener un alto nivel de integridad en sus procesos comerciales y en la ejecución del servicio o producto materia de la relación comercial con AGROBANCO.
b. **EL PROVEEDOR / CONTRAPARTE** se compromete y obliga, de manera expresa, incondicional e irrevocable, a no otorgar, donar y/o entregar obsequios, regalos y/o dinero u otros bienes de valor a los colaboradores de AGROBANCO para su beneficio u otros afines que vulneren los intereses de este último. Están exonerados de lo expuesto los productos perecibles, merchandising o de menor cuantía que no superen los US$ 50.00.
c. **AGROBANCO**, prohíbe estrictamente realizar las siguientes actividades:

- Los actos de corrupción, para retener u obtener negocios o lograr ventajas indebidas. No existen justificaciones o razones válidas que permitan tolerar o aceptar este tipo de conductas.
- Ofrecer, pagar, donar o dar dinero o bienes de valor a un funcionario público o tercero con el fin de obtener un beneficio indebido o negocios a favor de AGROBANCO.
- Los pagos de facilitación de trámites o atención de requerimientos u otros dirigidos a los colaboradores de AGROBANCO y/o funcionarios públicos con la finalidad de obtener un beneficio.
- Intentar inducir a un funcionario público o tercero, local o extranjero, a incumplir u omitir actos en contra de sus funciones, obligaciones y tomar decisiones vulnerando los procedimientos o normas vigentes, o realizar cualquier otro acto ilegal o no ético
- Inducir, no informar o permitir que se vulnere lo dispuesto en la presente declaración y la regulación vigente referente a los delitos mencionados u otros relacionados que puedan generar responsabilidad y un perjuicio reputacional a AGROBANCO.

15.3 El incumplimiento de la presente Cláusula por parte de **EL PROVEEDOR / CONTRAPARTE** genera la resolución del presente Contrato de pleno derecho, de conformidad con lo dispuesto en el artículo 1430 del Código Civil. **EL BANCO** mediante comunicación escrita notificará a **EL PROVEEDOR / CONTRAPARTE** la causal de resolución del Contrato, a su leal saber y entender. AGROBANCO se

reserva el derecho de ejecutar las acciones civiles y/o penales que pudiesen corresponder ante este incumplimiento**.**

15.4 La resolución del presente Contrato genera que **EL PROVEEDOR / CONTRAPARTE** no tenga derecho a reembolso, restitución, devolución o al pago por compensación o indemnización, ni pago de suma de dinero alguna por las inversiones o prestaciones realizadas durante la ejecución del presente Contrato; no pudiendo exigir a **AGROBANCO** ninguno de los conceptos antes mencionados.

15.5 Adicionalmente, y sin perjuicio de lo señalado en los numerales 15.3 y 15.4 de la presente Cláusula, **EL PROVEEDOR / CONTRAPARTE** declara, de manera expresa, incondicional e irrevocable que, en caso que este último, sus directores, gerentes y/o sus representantes, incumpla de manera parcial o total, alguna cualquiera de las obligaciones asumidas por **EL PROVEEDOR / CONTRAPARTE** en virtud de la presente Cláusula Décimo Quinta, **EL PROVEEDOR / CONTRAPARTE** libera y liberará de toda y cualquier responsabilidad, y asume la obligación de indemnizar y mantener indemne, e indemnizará y mantendrá indemne a AGROBANCO, por todo y cualquier daño o perjuicio que pudiera sufrir AGROBANCO, sus directivos, funcionarios, operadores, asesores, y/o empleados, así como cualquier bien o activo de su respectiva propiedad como resultado y en relación a cualquier daño y/o perjuicio, incluyendo pero sin limitarse a todos los daños y perjuicios causados por el incumplimiento de cualquier estipulación de la presente Cláusula, durante y/o en virtud de la ejecución del presente Contrato.

CLAUSULA DECIMO SEXTA: FISCALIZACIÓN

La ejecución de las prestaciones acordadas en el presente contrato a cargo de **EL CONTRATISTA** podrán ser objeto de revisión por parte de **LA ENTIDAD**, previa comunicación con un mínimo de 24 horas de anticipación, lo que incluye la posibilidad que dichas revisiones puedan ser efectuadas por sus Área de Auditoría Interna, Órgano de Control Institucional, su Sociedad de Auditoría Externa e incluso la Superintendencia de Banca, Seguros y AFP, de estimarlo necesario dicho ente supervisor.

Para estos efectos, **EL CONTRATISTA**, brindará a **LA ENTIDAD** la información necesaria para verificar el cumplimiento de prestaciones, debiendo también permitir la inspección de los servicios prestados por parte de cualquiera de los funcionarios y/o entidades señaladas en el párrafo anterior, si así fuere solicitado. Si producto de dichas revisiones se adviertas deficiencias, **EL CONTRATISTA** deberá coordinar con **LA ENTIDAD** un plazo prudente para subsanación y, si no hay acuerdo, **LA ENTIDAD** podrá determinar un plazo máximo para ello.

Si **EL CONTRATISTA** no permite la inspección y/o revisión sin causa justa, o no cumple con subsanar las diferencias que le fueran advertidas en los plazos establecidos, **LA ENTIDAD** podrá resolver el contrato de pleno derecho, constituyendo la presente una cláusula resolutoria expresa, de conformidad con lo previsto en el artículo 1430° del Código Civil.

CLÁUSULA DÉCIMO SEPTIMA: CONFIDENCIALIDAD

EL CONTRATISTA se compromete a mantener absoluta confidencialidad respecto de cualquier información que reciba o se desprenda del presente contrato, y en especial aquella vinculada con los clientes/prestatarios/colaboradores de **LA ENTIDAD**, su mecanismo de negocio u operativa. Será exclusiva responsabilidad de **EL CONTRATISTA** cualquier uso o abuso indebido de tal información. **EL CONTRATISTA** usará la Información Confidencial que **LA ENTIDAD** le otorgue única y exclusivamente para los fines de la ejecución de **EL CONTRATO**.

EL CONTRATISTA mantendrá toda la información proporcionada por **LA ENTIDAD** en estricto secreto y confidencialidad en todos los aspectos. Para estos efectos, **EL CONTRATISTA** no podrá divulgar, publicar, anunciar, ni pondrá a disposición de otro modo la Información Confidencial, total o parcialmente, a terceros de modo alguno, ya sea directa o indirectamente, y tomará todas las medidas que sean razonablemente necesarias o adecuadas con la finalidad de mantener dicha información en estricto secreto y confidencialidad. **EL CONTRATISTA** declara que hará extensiva y suya la presente obligación frente a sus funcionarios, empleados, servidores, red de distribuidores y terceros que tenga a bien destacar para el cumplimiento cabal del presente contrato.

EL CONTRATISTA se compromete a indemnizar con respecto a todas las pérdidas, responsabilidad, daños y costos y gastos razonables (incluyendo gastos legales) que **LA ENTIDAD** pueda incurrir o mantener como resultado del incumplimiento de este Acuerdo por parte de **EL CONTRATISTA** y/o sus Representantes, salvo que dicho incumplimiento se deba a mandato judicial o de la autoridad administrativa regulatoria.

La presente cláusula se mantendrá vigente de manera indefinida, independientemente del motivo de su finalización.

CLÁUSULA DÉCIMO OCTAVA: SOLUCIÓN DE CONTROVERSIAS

Las partes acuerdan que cualquier disputa, controversia o reclamo, sin excepción, que surja con relación a este Contrato, su interpretación, aplicación, ejecución, incumplimiento o terminación, incluyendo cualquier duda con respecto a su existencia, validez o terminación, se solucionará, en lo posible, mediante trato directo y de acuerdo a los principios de la buena fe y común intención de las partes. De no llegar a un acuerdo ambas partes se someterán al fuero de Arbitraje que se llevara a cabo en el Centro de Arbitraje de la Cámara de Comercio de Lima, a la que se someten las Partes de manera incondicional, siendo de aplicación supletoria el Decreto Legislativo No. 1071.

El plazo de duración del proceso arbitral no deberá exceder de treinta (30) días calendario contados desde la fecha de instalación del Tribunal Arbitral. El laudo arbitral tendrá carácter definitivo, obligatorio y vinculante para las Partes, sin ningún derecho de apelación y puede ser presentado para la ejecución del mismo ante cualquier tribunal competente.

No obstante lo anterior, en el caso de la ejecución de un laudo arbitral,u otro caso que se requiera la intervención de jueces del Poder Judicial o de sus tribunales, ambas Partes se someten a la jurisdicción de los jueces y tribunales del Cercado de Lima, para lo cual cada Parte renuncia a la jurisdicción de su domicilio.

CLÁUSULA DÉCIMO NOVENA: RIESGO OPERACIONAL

Las partes declaran tener conocimiento de lo dispuesto por la normativa sobre Gestión Integral de Riesgos aprobada por la Superintendencia de Banca, Seguros y AFP, que tiene por objeto que las empresas supervisadas puedan gestionar los riesgos operacionales asociados a la subcontratación, así como establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados.

El incumplimiento de las obligaciones asumidas por **EL CONTRATISTA**, en la presente cláusula, constituye causal de resolución del presente contrato.

CLAUSULA VIGÉSIMA. - SEGURIDAD INFORMÁTICA Y FÍSICA A SER APLICADAS:
Las Partes se obligan entre sí a respetar y velar por el cumplimiento de las normas de seguridad informática y física, definidas como aquellas directrices y medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de las Partes. En este sentido, todas las personas que laboren para las Partes o sean designadas por las mismas para trabajar en las actividades asociadas a la ejecución del objeto contractual

son responsables del adecuado uso de la información suministrada para tal fin, por lo cual se debe velar por su integridad, confidencialidad y disponibilidad de la misma forma como se velaría por la información propia. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

CLAUSULA VIGÉSIMA PRIMERA. - PROCEDIMIENTOS FRENTE A LA EVIDENCIA DE ALTERACIÓN O MANIPULACIÓN DE EQUIPOS O INFORMACIÓN (de corresponder:
Frente a la evidencia de alteración o manipulación de equipos o información, la Parte incumplida deberá presentar las justificaciones necesarias y tomar todas las medidas necesarias y pertinentes para reducir los perjuicios que dicha alteración o manipulación pueda llegar a causar al propietario de los equipos o información, igualmente deberá reportarlo en el término de la distancia, a la división de seguridad de la información o quien haga sus veces de su titular y solicitar, en el acto, instrucciones precisas de manejo de la situación , las cuales deberá cumplir estrictamente. El servicio, no puede ser suspendido, so pretexto de un hecho evidente o supuesto de manipulación de equipos o información.

CLAUSULA VIGÉSIMA SEGUNDA. - PLANES DE CONTINUIDAD DEL NEGOCIO:
En la medida en que el objeto del presente Contrato involucra la prestación de un servicio, es responsabilidad de **EL CONTRATISTA** preparar, actualizar periódicamente, y probar regularmente los planes de Contingencia, Emergencia y Recuperación, previendo la continuidad de los procesos críticos para el negocio, en el evento de presentarse una interrupción o degradación del servicio por cualquier causa.

En virtud de ello, **EL CONTRATISTA** se compromete a continuar prestando sus servicios a favor de **AGROBANCO** siempre que, no obstante haberse presentado los eventos inesperados, tenga la posibilidad fáctica de poder brindarlos.

CLAUSULA VIGÉSIMA CUARTA: NO EXISTENCIA DE VÍNCULO LABORAL:

Queda establecido que el presente Contrato no genera vínculo laboral alguno entre **EL CONTRATISTA** y **AGROBANCO** ni con personal que éste designe para la capacitación y coordinación con **AGROBANCO**, por lo tanto, no se genera ningún tipo de derechos laborales.

CLAUSULA VIGÉSIMA CUARTA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato y en el Reglamento de Contrataciones y Adquisiciones de AGROBANCO, se utilizarán las disposiciones pertinentes de la Ley de Contrataciones del Estado y su Reglamento y demás normativa especial que resulte aplicable y las disposiciones pertinentes del Código Civil vigente y demás normas concordantes.

CLAUSULA VIGÉSIMA QUINTA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLAUSULA VIGÉSIMA SEXTA: VERACIDAD DE DOMICILIOS

Las partes contratantes han declarado sus respectivos domicilios en la parte introductoria del presente contrato.

De acuerdo con las Bases, las ofertas técnico y económica y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de Lima al ……

"AGROBANCO"

"AGROBANCO"

"EL CONTRATISTA"

FORMATO N°01

REGISTRO DEL PARTICIPANTE

NIVEL DE CONTRATACION AL QUE SE PRESENTA:

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

Denominación del proceso: **ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS**

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.

Ciudad y fecha, ……

……..……..……..

Firma, Nombres y Apellidos del postor

ANEXO N°01
DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

El que suscribe, ……., identificado con DNI Nº ....., representante Legal de la empresa ....., con 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(s):		

Ciudad y fecha, ……

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

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

ANEXO N°02
DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL BIEN CONVOCADO

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración:

El que suscribe……. (postor y/o Representante Legal de .....), identificado con DNI Nº ....., RUC Nº ..... en calidad de postor, luego de haber examinado los documentos del proceso de la referencia proporcionados por la AGROBANCO, y conocer todas las condiciones existentes, el suscrito ofrece la **ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS**, de conformidad con dichos documentos y de acuerdo con los Requerimientos Técnicos Mínimos y demás condiciones que se indican en el Capítulo III de la sección específica de las Bases.

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

Ciudad y fecha, ……

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

(*) Adicionalmente, puede requerirse la presentación de otros documentos para acreditar el cumplimiento de los Requerimientos Técnicos Mínimos, conforme a lo señalado en el contenido del sobre técnico.

ANEXO N°03

DECLARACIÓN JURADA

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración:

El que suscribe, …… (postor y/o Representante Legal) de la empresa: ....., identificado con DNI Nº ....., RUC Nº ....., domiciliado en ....., que se presenta como postor de la **ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO,** para la **ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS**, declaro bajo juramento lo siguiente:

1. No haber incurrido y se obliga a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
2. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado.
3. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
4. Conozco, acepto y me someto a las Bases, condiciones y reglas del procedimiento de selección.
5. Soy responsable de la veracidad de los documentos e información que presente en el procedimiento de selección.
6. No haber tenido ningún vínculo laboral con el Banco en los últimos 12 meses.
7. Me comprometo a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.
8. 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.
9. Actualmente, no estoy siendo investigado y/o procesado (o lo estuvo anteriormente), por el delito de lavado de activos, financiamiento del terrorismo y/o delito precedente.

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 SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

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 oferta conjunta en la **ADQUISICIÓN NIVEL II Nº0024-2024-AGROBANCO "ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"**, 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 N°05
DECLARACION JURADA DE PROVEDORES Y CONTRAPARTES

REQUERIMIENTO DE INFORMACIÓN PARA PROVEEDORES Y CONTRAPARTES

En cumplimiento de la Resolución SBS N° 2660-2015 Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo y la Ley N° 30424 y sus modificatorias, que regula la Responsabilidad Administrativa de las Personas Jurídicas frente a los delitos de: (1) cohecho activo transnacional; (2) cohecho activo genérico; (3) cohecho activo específico; (4) lavado de activos y otros delitos vinculados a la minería ilegal y crimen organizado y (5) delitos de terrorismo; el Banco Agropecuario ha establecido determinados procedimientos como medios de prevención frente a los delitos antes señalados. En tal sentido, se solicita completar el siguiente cuestionario con el objeto de establecer un conocimiento adecuado de nuestros proveedores y contrapartes, al momento de iniciar nuestras relaciones contractuales.

Complemetar la información en letras **MAYÚSCULAS**.

1. DATOS DEL CLIENTE

NÚMERO DE RUC		**Tipo de contribuyente**	PERSONA JURÍDICA		DNI
NOMBRE O RAZÓN SOCIAL					
ACTIVIDAD ECONÓMICA 1					
ACTIVIDAD ECONÓMICA 2					
ACTIVIDAD ECONÓMICA 3					

2. DIRECCIÓN Y TELÉFONOS

DIRECC. OFICINA PRINCIPAL						**ID CIUDAD**	**Teléf. Fijo 1**	**Teléf. Fijo 2**
DEPARTAMENTO	ELIGE_DEPARTAMENTO	**PROVINCIA**	ELIGE_PROVINCIA	**DISTRITO**	ELIGE_DISTRITO			
Direccion de la sucursal 1								
DEPARTAMENTO	ELIGE_DEPARTAMENTO	**PROVINCIA**	ELIGE_PROVINCIA	**DISTRITO**	ELIGE_DISTRITO	**0**		
Direccion de la sucursal 2								
DEPARTAMENTO	ELIGE_DEPARTAMENTO	**PROVINCIA**	ELIGE_PROVINCIA	**DISTRITO**	ELIGE_DISTRITO	**0**		
Direccion de la sucursal 3								
DEPARTAMENTO	ELIGE_DEPARTAMENTO	**PROVINCIA**	ELIGE_PROVINCIA	**DISTRITO**	ELIGE_DISTRITO	**0**		

3. DATOS DEL O LOS REPRESENTANTES LEGALES (EN CASO DE EMPRESA)

Apellido Paterno	Apellido Materno	Nombres	Tipo de Doc. de Identidad	Número de Documento	Registra antecedentes penales	Cargo
			DNI		NO	OTRO
			DNI		NO	
			DNI		NO	OTRO
			DNI		NO	OTRO
			DNI		NO	OTRO

4. DATOS DE LOS DIRECTORES (EN CASO DE EMPRESA)					
Apellido Paterno	Apellido Materno	Nombres	Doc. de Identidad	Número de Documento	Registra antecedentes penales
			DNI		SI
			DNI		SI
			DNI		SI
			DNI		SI
			DNI		SI

5. DATOS DE LOS ACCIONISTAS, SOCIOS Y/O ASOCIADOS (EN CASO DE EMPRESA)						
Apellido Paterno	Apellido Materno	Nombres	Documento de Identidad	Número de Documento	Registra antecedentes penales	% de Participación
			DNI		NO	
			DNI		NO	
			DNI		NO	
			DNI		NO	
			DNI		NO	

6. DATOS DEL OFICIAL DE CUMPLIMIENTO Y/O RESPONSABLE DEL SISTEMA DE PREVENCIÓN DE DELITOS (DE SER EL CASO)						
Apellido Paterno	Apellido Materno	Nombres	Documento de Identidad	Número de Documento	Registra antecedentes penales	Cargo
			DNI		NO	
			DNI		NO	
			DNI		NO	

7. DATOS DE FUNCIONAMIENTO (EN CASO DE EMPRESA)	
Año de constitución	
Número de Licencia de Autorización	
Fecha de Licencia de Autorización	
Entidad Reguladora	
Capital Suscrito	

8. DATOS DEL CONTACTO							
Apellido Paterno	Apellido Materno	Nombres	Doc. de Identidad	Número de Documento	Telefono Celular	Correo electrónico	Cargo
			DNI				
			DNI				
			DNI				

9. LINEAMIENTOS DE ÉTICA Y CONDUCTA (EN CASO DE EMPRESA)	
¿La Empresa cuenta con un Código de Conducta y Ética?	
¿Qué órgano lo aprueba?	
¿Cuál es la fecha de su aprobación o última actualización?	
¿Se realizan auditorías internas o externas sobre el cumplimiento de los lineamientos de ética y conducta? Breve detalle y fecha de la última auditoría	

10. LINEAMIENTOS DE PREVENCIÓN DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO Y EL DECRETO LEGISLATIVO					
¿La Empresa cuenta con un Sistema de Prevención de Lavado de Activos y del Financiamiento del Terrorismo?					
¿La Empresa ha elaborado e implementado un Manual y un Código de Prevención de Lavado de Activos y del Financiamiento del Terrorismo?					
¿Qué órgano los aprueba?					
¿Cuál es la fecha de su aprobación o última actualización?					
¿La Empresa ha sido objeto de sanciones por motivos de LA/FT?		Ente sancionador:		Fecha:	
De ser afirmativa ¿Cuál es el estado de atención y/o subsanación de dicha sanción?					
¿Se realizan auditorías internas o externas sobre el cumplimiento de los lineamientos de ética y conducta? Breve detalle y fecha de la última auditoría.					

11. LINEAMIENTOS ANTICORRUPCIÓN					
¿La Empresa cuenta con un Modelo de Prevención de Delito (soborno)?					
¿Qué órgano los aprueba?					
¿Cuál es la fecha de su aprobación o última actualización?					
¿La Empresa ha sido objeto de sanciones por motivos de corrupción?		Ente sancionador:		Fecha:	
¿Se llevó a cabo la elaboración de un plan para mitigar o eliminar el hecho generardor de dicha sanción?					
¿Se realizan auditorías internas o externas sobre el cumplimiento de los lineamientos de ética y conducta? Breve detalle y fecha de la última auditoría.					

12. PROCESOS JUDICIALES			
¿La Empresa o alguno de sus representantes legales, funcionarios y/o directivos ha estado o se encuentra implicada en algún proceso judicial?			
Nombre y apellidos de la persona implicada		Detallar hecho y fecha	
Nombre y apellidos de la persona implicada		Detallar hecho y fecha	
Nombre y apellidos de la persona implicada		Detallar hecho y fecha	

DOCUMENTOS A ADJUNTAR	
En caso de correspnoder, remitir los documentos detallados a continuación:	**Comentarios**
Licencia de funcionamiento o resolución de autorización de funcionamiento	
Ficha RUC o DNI en copia (caso de persona natural)	
Listado de sus principales cinco (05) provedores.	
Listado de sus principales cinco (05) clientes.	

COMENTARIOS ADICIONALES

CERTIFICACIÓN
Declaro que:
1. Las actividades informadas y/o detalladas en el presente cuestionario no se encuentran vinculadas y/o asociadas a actividades al margen de la Ley; sino por el contrario, correspnoden al cumplimiento irrestricto de las normas y leyes que rigen nuestra sociedad.
2. La información brindada en la presente Declaración Jurada es real y que, en caso de detectarse fraude y/o falsedad en la misma o la omisión de información solicitada, estaré sujeto a las sanciones administrativas establecidas en la legislación vigente sobre la materia, sin perjuicio de la responsabilidad personal y/o penal que corresponda o la rescisión y/o resolución del contrato celebrado.

Firma del Representante Legal	**Firma del Representante Legal**

ANEXO Nº06

DECLARACIÓN JURADA SOBRE PLAZO DE ENTREGA DEL BIEN

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración,

Por medio de la presente, el que suscribe, don ……, identificado con D.N.I. N° ……., **DECLARO BAJO JURAMENTO** que mi representada se compromete a ejecutar la **"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"**, de acuerdo al siguiente detalle:

- El plazo de entregade las licencias hasta 15 días calendarios contado a partir del día siguiente de la firma del contrato.
- El plazo máximo para la implementación de realizará hasta los 60 días calendarios contados a partir de la conformidad de la entrega de las licencias.
- El plazo de la etapa de operación es de 12 meses contados a partir de de la conformidad de la etapa de implementación.

Ciudad y fecha, ……

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

ANEXO N°07

DECLARACION JURADA DE GARANTIA

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO,** que mi representada se compromete a:

h) Los componentes deberán ser nuevos y originales según el número de parte del fabricante. No se aceptarán componentes de mercado secundario o refurbished.
i) Presentar carta del fabricante que se indique que los componentes son nuevos y originales.
j) Todo el equipamiento (hardware y software) debe contar con garantía de fábrica y del mi representada por …….. **(Indicar mejora, mínimo 01 año de acuerdo con bases)** a partir de la conformidad del servicio de la puesta en operación de la solución, emitida por la División de Infraestructura, Producción y Soporte, con alcance de 24 horas del día, los 7 días de la semana, los 365 días del año.
k) Los repuestos, mano de obra.
l) Otros que puedan incurran por el servicio brindado, serán sin costo adicional para AGROBANCO.
m) No alegar inconvenientes con el fabricante para la provisión de los trabajos de asistencia técnica mencionados, debiendo garantizar en toda circunstancia la posibilidad de escalamiento de estos eventos.
n) Gestionar la reposición de los componentes o partes que se requieran para la reparación de los equipos proporcionados en caso estos los requiera.
o) Cuando se tenga la necesidad de cambiar un equipo, este será recogido de la oficina principal de AGROBANCO

Ciudad y fecha, ……

Nota: El postor deberá adjuntar el documento que acredite la garantía solicitada, el cual deberá estar vigente al día de la presentación de propuestas.

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

ANEXO N°08

DECLARACIÓN JURADA DE REPRESENTACIÓN PARA LA COMERCIALIZACIÓN DE LAS LICENCIAS ANTISPAM Y ANTIVIRUS

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO**, que que mi representada se compromete a presentar un documento emitido por el fabricante, en el cual se acredite que está autorizado para comercializar licencias, mantenimiento de licencias, mantenimiento de licencias, soporte técnico y suscripción de licencias de antispam y antivirus.

Ciudad y fecha, ……

Nota: El postor deberá adjuntar el documento emitido por el fabricante que acredite la autorización para la comercialización de las licencias antispam y antivirus.

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

ANEXO N°09

DECLARACION JURADA DE PERSONAL PROPUESTO

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO**, que mi representada se compromete a presentar EL SIGUIENTE PERSOAL CLAVE PROPUESTO

CARGO	NOMBRE DEL PERSONAL PROPUESTO	REQUISITOS	EXPERIENCIA MINIMA
UN JEFE DE PROYECTO	…… (Indicar nombre, apellidos y DNI del jefe de proyecto propuesto)	1. Título profesional en Ingeniería de Sistemas o Ingeniería de Sistemas e Informática, Ingeniería de Telecomunicaciones o Ingeniería Industrial o Ingeniería de Seguridad y Auditoría Informática o Ingeniería Electrónica o Ingeniería Informática o carreras afines a las tecnologías de la Información. **2. Colegiado y habilitado al momento de la presentación de la propuesta. (Indicar CIP)** 3. Certificado de Project Management Profesional (PMP) Vigente ó Curso de Gerencia de Proyecto con mínimo de 240 horas de instrucción (Horas Cronológicas) 4. Certificado en ITIL, mínimo v3.	Experiencia mínima de **tres (03) años** como jefe de proyectos de soluciones de seguridad informática
UN ESPECIALISTA DE SOLUCION ANTIVIRUS	…… (Indicar nombre, apellidos y DNI del especialista de solución antivirus propuesto)	1. Mínimo bachiller ó profesional en Ingeniería de Sistemas e Informática o Ingeniería de Telecomunicaciones o Ingeniería de Electrónica o Ingeniería de Seguridad y Auditoría Informática o Técnico en seguridad informática o Técnico en Redes y Comunicaciones de Datos, o afines a las Tecnologías de la Información.	Experiencia no menor de dos (02) en la implementación, soporte técnico y mantenimiento de soluciones de protección de endpoint y servidores

CARGO	NOMBRE DEL PERSONAL PROPUESTO	REQUISITOS	EXPERIENCIA MINIMA
		2. Debe contar con Certificación vigente en el producto ofertado.	
UN ESPECIALISTA DE SOLUCION ANTISPAM	…… (Indicar nombre, apellidos y DNI del especialista de solución antispam propuesto)	1. Mínimo bachiller ó profesional en Ingeniería de Sistemas e Informática, Ingeniería de Telecomunicaciones, Ingeniería de Electrónica, Ingeniería de Seguridad y Auditoría Informática, Técnico en seguridad informática, Técnico en Redes y Comunicaciones de Datos, o afines. 2. Deben contar con Certificación vigente en el producto ofertado	Experiencia no menor de dos (02) en la implementación, soporte técnico y mantenimiento de soluciones de protección de correo electrónico.

Ciudad y fecha, ……

Nota: El postor deberá adjuntar el CV documentado (certificados de estudios, colegiatura, constancias de trabajo, ETC.) que acredite fehacientemente el cumplimiento de los requisitos mínimos solicitados del personal clave.

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

ANEXO N°10

DECLARACION JURADA DE CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTOS

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO**, que mi representada se compromete a:

1. Brindar una capacitación de transferencia de conocimientos sobre la configuración y administración de la solución al personal de la Gerencia de Transformación Digital e Innovación que se deberá realizar dentro de los sesenta (60) días siguientes a la conformidad de la etapa 1.

2. Asi mismo esta capacitación será de 03 horas para hasta 4 personas quien deberá entregar un syllabus con los temas a tratar, los mismos que deberán ser aprobados por la ENTIDAD mediante un correo electrónico enviado por el Especialista de Infraestructura y Producción de la ENTIDAD y/o Jefe de Infraestructura, Producción y Soporte.

3. Provisionar a Agrobanco manuales de usuario, guías de configuración y procedimientos operativos estándar.

4. Me comprometo a entregar certificados de participación, firmados por el personal capacitador a los participantes de la capacitación.

Ciudad y fecha, ……

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

ANEXO N°11

DECLARACION JURADA DE ATENCIÓN DE SOPORTE Y MANTENIMIENTO

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO**, que mi representada se compromete en caso de ser adjudicado a cumplir con lo siguiente:

1. **Soporte técnico:**

a) Contar con una Mesa de ayuda como un único punto de contacto para atender cualquier requerimiento y/o incidente y estar en la capacidad de dar soporte y solución a los incidentes que son reportados.

b) Contar con una bolsa de 80 horas adicionales de soporte local para atender incidentes y requerimientos derivados del proceso de implementación.

c) En el caso que las horas adicionales no se hayan utilizado durante el año, podrán usarse para capacitaciones las mismas que serán acordadas entre el POSTOR y el jefe de la División de Infraestructura Producción y Soporte.

d) Contar con soporte técnico integral para las soluciones ofertadas (en hardware y software) que incluya actualizaciones de software, reparaciones, reemplazos y otros de hardware que garanticen mantener siempre operativa la solución implementada.

e) El acceso a la mesa de ayuda para la generación de una atención de servicio debe contener como mínimo:
   - Poder realizar un requerimiento mediante llamada local.
   - Mediante el envío de un correo electrónico.
   - Mediante el uso de un formulario web definido por el postor.

f) Todo incidente de orden técnico o funcional es atendido en un primer nivel el POSTOR local y de requerir escalar al fabricante, será a través del POSTOR, el cual realizará los contactos con el fabricante.

g) Dependiendo de la complejidad de la incidencia, la atención en primera instancia podrá ser vía telefónica con el soporte técnico local, si no es posible la solución por este medio, podrá ser vía acceso remoto y en una tercera instancia será la visita de técnicos a las oficinas de Agrobanco.

h) Cuando se presente una situación excepcional que le impida cumplir con el tiempo estipulado para la solución, Mi representada podrá enviar una Carta y/o correo electrónico a la División de Infraestructura, Producción y Soporte exponiendo los motivos que originaron la situación, con la finalidad de evaluar las justificaciones.

i) Las licencias y el soporte de fabricante deben cubrir reemplazos de equipos y soporte por el periodo de 1 año contados a partir de la firma de conformidad del servicio implementado.
j) Como parte del servicio, Mi representada debe ser capaz de gestionar y responder ante incidentes. Para ello el proveedor debe contar con una solución de tipo SIEM (Security Information Event Management) que le permita detectar, responder y neutralizar las amenazas informáticas que sean detectadas por las soluciones que formarán parte del presente servicio: Antivirus y Antispam, incluyendo la solución de filtro web Barracuda presente en el banco.

2. Mantenimiento:

a) Mi representada realizará 1 mantenimiento de las soluciones adquiridas en coordinación con el BANCO al 6to mes de iniciado el servicio contratado, debiendo detallar las actividades a ejecutar.
b) Mi representada deberá presentar el rol del mantenimiento con el detalle de las actividades a ejecutar el mismo que deberá ser proporcionado al culminar la fase de implementación.
c) Mi representada notificará al personal de la división de Infraestructura con 30 días de antelación del inicio del mantenimiento.
d) El personal de mi representada que realizará el mantenimiento deberá contar con las características del perfil técnico indicadas en el literal III (relacionado al personal).

Ciudad y fecha, ……

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

ANEXO N°12

DECLARACION JURADA DE SOLUCIÓN OFERTADA

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración, El que suscribe, don _____identificado con D.N.I N° _____Representante Legal de _____, con RUC N° _____, **DECLARO BAJO JURAMENTO**, que mi representada se compromete a que las licencias Antispam y Antivirus son compatibles con lo especificado y requerido en las especificaciones técnicas estipulados en el numeral IV del Capítulo III, de la sección Específica de las presentes bases.

Ciudad y fecha, ……

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

ANEXO N°13

EXPERIENCIA DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

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	N° Contrato o factura	Importe del contrato o factura	Fecha de inicio y término
1					
2					
3					
4					
5					
6					
7					
8					
9					
10 . . .	. . . .	. . . .	. . . .	. . . .	. . . .
TOTAL					

Ciudad y fecha, ……

Nota. - Con la finalidad de acreditar fehacientemente la experiencia el postor deberá adjuntar copias de contratos con sus respectivas constancias de prestación del servicio o facturas con sus constancias de abono haciendo referencia a la factura informada o movimientos de su estado de cuenta haciendo referencia a la factura informada.

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

ANEXO Nº14

OFERTA ECONÓMICA

(MODELO)

Señores
COMITÉ DE SELECCIÓN
ADQUISICIÓN NIVEL II Nº 024-2024-AGROBANCO
"ADQUISICION DE LICENCIAS ANTISPAM Y ANTIVIRUS"

Presente.-

De nuestra consideración,

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

CONCEPTO	CANTIDAD UND.	Precio Unitario Incl. IGV S/.	Precio Total Incl. IGV S/.
Adquisición de Licencias Anti virus	1700		
Adquisición de Licencias Anti spam	1000		
Implementación (Etapa 2)			
Soporte y Mantenimiento (Etapa 3)			
Monto Total Incl. IGV S/.			**S/…….**

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

Ciudad y fecha, ……

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