SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC]	Es una indicación que debe ser completada o eliminada por la entidad contratante durante la elaboración de las bases conforme a las instrucciones brindadas.
2	**[ABC]**	Es una indicación o información que debe ser completada por la entidad contratante con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	**Advertencia** • **Abc**	Se refiere a advertencias a tener en cuenta por los evaluadores y los proveedores. No deben ser eliminadas.
4	**Importante para la entidad contratante** • ***Xyz***	Se refiere a consideraciones importantes a tener en cuenta por los evaluadores y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases deben ser elaboradas en formato WORD, y deben tener las características del presente documento. De existir algún cambio en el formato como márgenes, fuente, tamaño de letra, entre otros, no acarrea su nulidad, salvo que por el tipo o tamaño de letra impida la lectura por parte de los proveedores.

INSTRUCCIÓN DE USO:

Una vez registrada la información solicitada dentro de los corchetes, el texto debe quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.

BASES INTEGRADAS

LICITACIÓN PÚBLICA ABREVIADA PARA BIENES

LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC

CONTRATACIÓN DE BIENES

ADQUISICIÓN DE LICENCIAS SOFTWARE ANTIVIRUS PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LOS SERVIDORES DEL CENTRO DE DATOS PARA ASEGURAR LA CONTINUIDAD OPERATIVA DE LA UNIVERSIDAD, ASÍ COMO LA PROTECCIÓN DE TODAS LAS COMPUTADORAS DE LA UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

JUNIO - 2025

SECCIÓN GENERAL

DISPOSICIONES COMUNES DE LA LICITACIÓN PÚBLICA ABREVIADA PARA BIENES

(ESTA SECCIÓN NO DEBE SER MODIFICADA EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD)

CAPÍTULO I
ASPECTOS GENERALES

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 32069, Ley General de Contrataciones Públicas, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

1.2. ALCANCE

La presente base estándar correspondiente al procedimiento de selección de licitación pública abreviada para bienes se utiliza por la entidad contratante para lo siguiente: i) la adquisición de bienes según la cuantía establecida en la Ley de Presupuesto del Sector Público para el Año Fiscal correspondiente, ii) la adquisición de bienes homologados, iii) la adquisición de bienes de rehabilitación y reconstrucción posterior emergencias y desastres, iv) la segunda convocatoria de una licitación pública para bienes o bienes especializados, o v) se trate de insumos directamente utilizados en los procesos productivos por las empresas del Estado conforme la Séptima Disposición Complementaria Final de la Ley.

CAPÍTULO II
DESARROLLO DEL PROCEDIMIENTO DE SELECCIÓN

2.1 ETAPAS DE LA LICITACIÓN PÚBLICA ABREVIADA PARA BIENES

Las etapas del presente procedimiento de selección son las siguientes:

ETAPA	CARACTERÍSTICAS	BASE LEGAL
a) Convocatoria	Se realiza a través del SEACE de la Pladicop en la fecha señalada en el cronograma.	Artículos 63 y 64 del Reglamento.
b) Registro de participantes	Aplica lista abierta, por lo que cualquier proveedor puede registrarse como participante en el procedimiento de selección.	Artículos 65 y 93 del Reglamento.
c) Cuestionamientos a las bases (consultas, observaciones e integración)	1. La presentación de consultas y observaciones se realiza en un plazo no menor a tres días hábiles contabilizados desde el día siguiente de la convocatoria. 2. La absolución de los referidos cuestionamientos y la publicación de las bases integradas se realiza en la fecha prevista en el cronograma del procedimiento de selección.	Artículos 66, y 93 del Reglamento.
d) Evaluación de ofertas técnicas y económicas	1. La presentación de ofertas se realiza a través del SEACE de la Pladicop en un plazo no menor de tres días hábiles contabilizados desde la publicación de la integración de bases. 2. Las ofertas son presentadas por los participantes desde las 00:01 horas hasta las 23:59 horas del día (hora peruana), según el cronograma del procedimiento de selección; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo con lo requerido en las bases. 3. La evaluación de ofertas es SIN PRECALIFICACIÓN y consiste en: a. Admisión de las ofertas: Los evaluadores revisan que la oferta contenga los documentos señalados en el Capítulo II de la Sección Específica de las bases, caso contrario la oferta se considera no admitida. b. Revisión de los requisitos de calificación: Los evaluadores califican a los postores verificando que cumplan con los requisitos de calificación detallados en el Capítulo III de la Sección Específica de las bases. c. Evaluación técnica: Los evaluadores aplican los factores de evaluación previstos en el Capítulo IV de la Sección Específica de las bases a las ofertas que cumplen los requisitos de calificación. La evaluación de	Artículos 68, 72, 73, 74, 75 y 78 del Reglamento.

	la oferta económica es simultánea a la evaluación técnica, por lo cual la oferta económica es un factor de evaluación. 4. Todos los actos se realizan a través del SEACE de la Pladicop, incluyendo la subsanación de ofertas.	
***e)* Otorgamiento de la buena pro**	1. Definida la oferta ganadora, los evaluadores otorgan la buena pro, mediante su publicación en el SEACE de la Pladicop, incluyendo los documentos que sustenten los resultados de la admisión, calificación, evaluación y el otorgamiento de la buena pro. 2. En caso de haber sorteo por desempate, éste se realiza a través del SEACE de la Pladicop. 3. En caso se hayan presentado dos o más ofertas, el consentimiento de la buena pro es publicado a través del SEACE de la Pladicop al día siguiente de vencido el plazo correspondiente para interponer recurso de apelación, sin que los postores hayan ejercido el derecho de interponer dicho recurso. En caso de que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.	Artículos 80, 81, 82, 83 y 84 del Reglamento.

2.2 EVALUACIÓN DE OFERTAS ECONÓMICAS QUE SUPEREN LA CUANTÍA DE LA CONTRATACIÓN

2.1.1. En caso la oferta económica del postor que obtiene el mejor puntaje total supere la cuantía de la contratación, se siguen los siguientes pasos:

a) La DEC gestiona la solicitud de la ampliación de la certificación o previsión presupuestal correspondiente. De otorgarse ampliación, se procede a adjudicar la buena pro.
b) De no contar con la ampliación de la certificación o previsión presupuestal, los evaluadores negocian con el postor que obtuvo el mejor puntaje total la reducción del monto o la reducción de las prestaciones o condiciones del requerimiento, conforme al numeral 132.1 del artículo 132 del Reglamento.
c) En caso el postor con el mejor puntaje no acepte, se procede a negociar con los siguientes postores en el orden de prelación que obtuvieron. Si el postor que procede en el orden de prelación ofertó un monto por debajo de la cuantía de la contratación, se le adjudica la buena pro.
d) En caso el postor que obtuvo el mejor puntaje total reduzca su oferta económica pero la reducción no se encuentre dentro de la cuantía del la contratación de selección, se solicita la ampliación de la certificación de crédito presupuestario y/o previsión presupuestal correspondiente. En caso se otorgue la ampliación, se adjudica la buena pro. Caso contrario, se puede optar por: negociar con los siguientes postores en el orden de prelación o declarar desierto el procedimiento de selección.
e) Las decisiones adoptadas por los evaluadores en la negociación constan en actas que se publican en el SEACE de la Pladicop y se sustentan en el principio de valor por dinero, priorizando el cumplimiento de la finalidad pública de la contratación.

2.3 CONSIDERACIONES PARA TODOS LOS PROVEEDORES:

2.3.1 Para registrarse como participante en un procedimiento de selección convocado por una entidad contratante, es necesario que los proveedores cuenten con inscripción vigente ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Especializado para las Contrataciones Públicas Eficientes (OECE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.rnp.gob.pe.

2.3.2 Los proveedores que deseen registrar su participación deben ingresar al SEACE de la Pladicop utilizando su certificado (usuario y contraseña).

2.3.3 No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada, aun cuando el requerimiento haya sido homologado parcialmente respecto a las características técnicas y/o requisitos de calificación y/o condiciones de ejecución. Las consultas y observaciones que se formulen sobre el particular se tienen como no presentadas.

2.3.4 Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales).. No se acepta insertar la imagen de una firma. Las ofertas se presentan foliadas en todas sus hojas. El postor, el representante legal, apoderado o mandatario designado se hace responsable de la totalidad de los documentos que se incluyen en la oferta. El postor es responsable de verificar, antes de su envío, que el archivo pueda ser descargado y su contenido sea legible.

2.3.5 En el caso que el proveedor, al registrarse como participante, presente una declaración jurada de desafectación del impedimento debido a parentesco establecido en el inciso 2 del numeral 30.1 del artículo 30 de la Ley, se debe incluir como requisito adicional de admisión de su oferta la acreditación documental de su condición de desafectación, conforme a lo señalado en el numeral 39.4 del artículo 39 del Reglamento.

2.4 CONSIDERACIONES ADICIONALES PARA LOS CONSORCIOS:

2.4.1 En el caso de consorcios, basta que uno de sus integrantes se haya registrado como participante en el procedimiento de selección, para lo cual dicho integrante debe contar con inscripción vigente en el RNP como proveedor de bienes. Los demás integrantes del consorcio deben contar con inscripción vigente en el RNP, en las demás etapas del procedimiento de selección. No se considera consorcio a la asociación de personas de duración ilimitada o indefinida que, denominándose consorcios, han sido constituidas como personas jurídicas en los Registros Públicos.

2.4.2 Los integrantes de un consorcio no pueden presentar ofertas individuales ni conformar más de un consorcio en un procedimiento de selección, o en un determinado ítem cuando se trate de procedimientos de selección según relación de ítems. Tratándose de un procedimiento por relación de ítems, los integrantes del consorcio pueden participar en ítems distintos al que se presentaron en consorcio, sea en forma individual o en consorcio.

2.4.3 Como parte de los documentos de su oferta el consorcio debe presentar la promesa de consorcio con firmas digitales de todos sus integrantes, o en su defecto, firmas legalizadas, de ser el caso, en la que se consigne lo siguiente:

a) La identificación de los integrantes del consorcio. Se debe precisar el nombre completo o la denominación o razón social de los integrantes del consorcio, según corresponda.
b) La designación del representante común de consorcio.
c) El domicilio común del consorcio.
d) El correo electrónico común del consorcio, al cual se dirigirán todas las comunicaciones remitidas por la entidad contratante al consorcio durante el proceso de contratación, siendo éste el único válido para todos los efectos.
e) Las obligaciones que correspondan a cada uno de los integrantes del consorcio.

f) El porcentaje del total de las obligaciones de cada uno de los integrantes, respecto del objeto del contrato. Dicho porcentaje debe ser expresado en número entero, sin decimales.

2.4.4 La información contenida en los literales a), e) y f) precedentes no puede ser modificada, con ocasión de la suscripción del contrato de consorcio, ni durante la etapa de ejecución contractual. En tal sentido, no cabe variación alguna en la conformación del consorcio, por lo que no es posible que se incorpore, sustituya o separe a un integrante.

2.4.5 El representante común tiene facultades para actuar en nombre y representación del consorcio, en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con poderes suficientes para ejercitar los derechos y cumplir las obligaciones que se deriven de su calidad de postor y de contratista hasta la conformidad o liquidación del contrato, según corresponda. El representante común no debe encontrarse impedido, inhabilitado ni suspendido para contratar con el Estado. Para cambiar al representante común, todos los integrantes del consorcio deben firmar (mediante firmas legalizadas o firmas digitales) el documento en el que conste el acuerdo, el cual surte efectos cuando es notificado a la entidad contratante.

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales).

2.4.6 En el caso de consorcios las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el representante común o por todos los integrantes del consorcio, según corresponda (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales). En el caso de los documentos que deban suscribir todos los integrantes del consorcio, la firma es seguida de la razón social o denominación de cada uno de ellos. Lo mismo aplica en caso deban ser suscritos en forma independiente por cada integrante del consorcio, de acuerdo con lo establecido en los documentos del procedimiento de selección. En el caso de un consorcio integrado por una persona natural, bastará que la persona natural indique debajo de su firma, sus nombres y apellidos completos.

2.4.7 La acreditación del requisito de calificación de la experiencia del postor se realiza en base a la documentación aportada por los integrantes del consorcio que se hubieran comprometido a ejecutar conjuntamente las obligaciones vinculadas directamente al objeto materia de la contratación, de acuerdo con lo declarado en la promesa de consorcio. Para ello se debe seguir los siguientes pasos:

a) Primer paso: obtener el monto de facturación por cada integrante del consorcio, el cual se obtiene de la sumatoria de montos facturados por éste que, a criterio del evaluador han sido acreditados conforme a las bases, correspondiente a las contrataciones ejecutadas en forma individual y/o consorcio.

   En caso un integrante del consorcio presente facturación de contrataciones ejecutadas en consorcio, se considera el monto que corresponda al porcentaje de las obligaciones del referido integrante consorcio. Este porcentaje debe estar consignado expresamente en la promesa o en el contrato de consorcio, de lo contrario, no se considera la experiencia ofertada en consorcio.

b) Segundo paso: verificar que el integrante del consorcio que acredita la mayor experiencia cumpla con un determinado porcentaje de participación. En caso la entidad contratante haya establecido en las bases un porcentaje determinado de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, debe verificarse que éste cumple con dicho parámetro a efectos de considerar su experiencia.

c) Tercer paso: sumatoria de experiencia de los consorciados. Para obtener la experiencia del consorcio se suma el monto de facturación aportado por cada integrante que cumple con lo señalado previamente.

2.4.8 Para calificar la experiencia del postor no se toma en cuenta la documentación presentada por el o los consorciados que asumen las obligaciones referidas a las siguientes actividades:

i) Actividades de carácter administrativo o de gestión como facturación, financiamiento, aporte de garantías, entre otras.

ii) Actividades relacionadas con asuntos de organización interna, tales como representación u otros aspectos que no se relacionan con la ejecución de las prestaciones, entre otras.

Tratándose de bienes, solo se consideran las obligaciones vinculadas directamente al objeto de la contratación, como la fabricación y/o comercialización. No corresponde considerar la experiencia presentada por los integrantes del consorcio que se obliguen a ejecutar las demás actividades de la cadena productiva y actividades accesorias, tales como el aporte de materias primas, combustible, infraestructura, transporte, envasado, almacenaje, entre otras.

2.4.9 Los integrantes de un consorcio se encuentran obligados solidariamente a responder frente a la entidad contratante por los efectos patrimoniales que ésta sufra como consecuencia de la actuación de dichos integrantes, ya sea individual o conjunta, durante el procedimiento de selección y la ejecución contractual.

CAPÍTULO III
RECURSO DE APELACIÓN

3.1. ACCESO AL EXPEDIENTE DE CONTRATACIÓN

Una vez otorgada la buena pro, la dependencia encargada de las contrataciones está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, con excepción de la información calificada como secreta, confidencial o reservada por la normativa de la materia y de aquella correspondiente a las ofertas que no fueron admitidas, a más tardar dentro del día hábil siguiente de haberse solicitado por escrito.

A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la entidad contratante debe entregar dicha documentación en el menor tiempo posible, previo pago de la tasa por tal concepto previsto en el Texto Único de Procedimientos Administrativos (TUPA) de la respectiva entidad contratante.

3.2. RECURSO DE APELACIÓN

A través del recurso de apelación se pueden impugnar los actos dictados durante el desarrollo del procedimiento de selección hasta antes del perfeccionamiento del contrato, incluyendo aquellos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por la entidad contratante que afecten la continuidad de éste.

El recurso de apelación se presenta ante la mesa de partes digital o física del Tribunal de Contrataciones Públicas o de la entidad contratante, según corresponda, según corresponda.

3.3. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone, como máximo, dentro de los cinco días hábiles siguientes de haberse notificado el otorgamiento de la buena pro a través del SEACE de la Pladicop

En el caso de la apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento de selección, el plazo indicado en el párrafo precedente se contabiliza desde que se toma conocimiento del acto que se desea impugnar. Se considera que se ha tomado conocimiento en el día de la publicación en el SEACE de la Pladicop del acto que se desea impugnar.

CAPÍTULO IV
DEL CONTRATO

4.1 REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO:

Para perfeccionar el contrato, el proveedor o proveedores adjudicados presentan los siguientes requisitos de conformidad con el artículo 88 del Reglamento:

REQUISITO	CONSIDERACIONES ADICIONALES	BASE LEGAL
a) Garantías, salvo casos de excepción.	En los contratos de bienes, el postor ganador de la buena pro presenta una garantía de fiel cumplimiento por una suma equivalente al 10% del monto del contrato original. La garantía de fiel cumplimiento puede ser: (i) fideicomiso, solo en caso el plazo de ejecución del contrato supere los 90 días calendario, (ii) carta fianza financiera, (iii) contrato de seguro o (iv) retención de pago. Asimismo, en la sección especifica de las Bases puede considerarse la presentación de: i) garantía de fiel cumplimiento de prestaciones accesorias y, ii) garantía por adelantos directos, siempre que se cumplan las condiciones señaladas en el Reglamento. La retención de pago como garantía de fiel cumplimiento o de prestaciones accesorias aplica para ítems cuya cuantía adjudicada sea igual o menor a S/ 480 000,00 (cuatrocientos ochenta mil y 00/100 soles) en el caso de bienes. En el caso de las micro y pequeñas empresas estas pueden otorgar como garantía de fiel cumplimiento la retención de pago por parte de la entidad contratante con independencia de la cuantía de la contratación. **Excepciones:** Conforme a lo dispuesto en el literal a) del artículo 139 del Reglamento, en los contratos de bienes cuyos montos sean menores o iguales a 50 UIT, no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Esta excepción no aplica cuando la sumatoria de los contratos derivados de procedimientos de selección por relación de ítems, adjudicados a un mismo postor, superen el monto señalado. Asimismo, tampoco se otorga garantía de fiel cumplimiento en caso el objeto contractual sea la adquisición de bienes inmuebles de propiedad privada.	Numerales 61.4 y 61.5 del artículo 61 de la Ley. Artículos 88, 113, 114, 115, 116, 138 y 139 del Reglamento.

b) Contrato de consorcio, de ser el caso.	Cuando el postor ganador de la buena pro sea un consorcio, el contrato de consorcio se formaliza mediante documento privado, el cual debe cumplir con los siguientes requisitos: a. Contener la información mínima indicada en el numeral 2.3.3 del Capítulo II de la Sección General de las presentes bases. b. Identificar al integrante del consorcio a quien se efectuará el pago y emitirá la respectiva factura o, en caso de llevar contabilidad independiente, señalar el Registro Único de Contribuyentes (RUC), del consorcio. c. Consignar las firmas legalizadas ante notario público de cada uno de los integrantes del consorcio, de sus apoderados o de sus representantes legales, según corresponda. Lo indicado no excluye la información adicional que pueda consignarse en el contrato de consorcio con el objeto de regular su administración interna, como es el régimen y los sistemas de participación en los resultados del consorcio, al que se refiere el artículo 448 de la Ley N° 26887, Ley General de Sociedades. En ningún caso puede aceptarse la presentación de la promesa de consorcio que fue parte de la oferta, independientemente de que dicha promesa contenga firmas legalizadas ante notario.	Literal b) del artículo 88 del Reglamento.
c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de cuenta bancaria y nombre de la entidad bancaria en el exterior.	El CCI es requisito indispensable para realizar una transferencia entre cuentas de bancos diferentes, requerido para efectuar el pago a los proveedores domiciliados en el Perú. Para los proveedores no domiciliados, corresponde el número de cuenta bancaria y nombre de la entidad bancaria en el exterior.	Artículo 67 de la Ley. Artículo 88, del Reglamento.
d) Documento que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.	Corresponde a la vigencia del poder del representante legal que acredite que cuenta con facultades para perfeccionar el contrato. Asimismo, corresponde que el representante legal presente copia de su DNI. En el caso de personas naturales, se solicita la copia del DNI del postor.	Literal d) del numeral 88.1 del artículo 88 del Reglamento.

	En el caso de consorcios, estos documentos deben ser presentados por cada uno de los integrantes del consorcio que suscriban la promesa de consorcio, según corresponda.	
e) Institución Arbitral elegida por el postor, de corresponder.	Este requisito es obligatorio para todos los contratos que superen las 10 UIT[1]. Desde el 1 de enero de 2026, la institución arbitral elegida debe encontrarse inscrita en el Registro de Instituciones Arbitrales y Centros de Administración de Juntas de Prevención y Resolución de Disputas (REGAJU).	Artículos 77, 83 y 84 así como la Décima Disposición Complementaria Transitoria de la Ley. Artículo 88 del Reglamento.
f) Centro de administración de la JPRD elegida por el postor, de corresponder.	Solo procede este requisito cuando el contrato tenga como objeto el suministro de bienes y supere S/ 10 000 000,00 (diez millones y 00/100 soles) y adicionalmente se haya determinado la JPRD como medio de solución de controversias en la estrategia de contratación.	Artículos 77 y 79, así como Décima Disposición Complementaria Transitoria de la Ley. Artículos 88 y 346 del Reglamento

4.2 PERFECCIONAMIENTO DEL CONTRATO

El postor ganador de la buena pro debe presentar los requisitos para perfeccionar el contrato dentro del plazo de ocho o cinco días hábiles, según corresponda, contabilizados desde el día siguiente al registro del consentimiento de la buena pro en el SEACE de la Pladicop o de que ésta haya quedado administrativamente firme, de conformidad con el procedimiento y plazos dispuestos en los artículos 88, 89, 90 y 91 del Reglamento.

4.3 CONSIDERACIONES PARA LOS CONSORCIOS

4.3.1 Las garantías que presenten los consorcios para el perfeccionamiento del contrato durante la ejecución contractual y para la interposición de los recursos impugnativos, además de cumplir con las condiciones establecidas en la Ley y el Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no pueden ser aceptadas por las entidades contratantes o el Tribunal de Contrataciones Públicas. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio.

4.3.2 Para que un consorcio solicite la retención del 10% del monto del contrato original en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 114 del Reglamento, todos los integrantes del consorcio deben acreditar en su oferta la condición de micro o pequeña empresa, sin perjuicio que puedan acreditarlo al momento del perfeccionamiento del contrato

4.4 CONSIDERACIONES PARA LAS GARANTÍAS FINANCIERAS

4.4.1 En caso de garantías financieras, estas deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la respectiva entidad contratante

[1] De conformidad con el numeral 84.1 del artículo 84 de la Ley, el arbitraje puede ser ad hoc solo en los casos en los que el monto de la controversia no supere las diez UIT.

bajo responsabilidad de las empresas que las emiten. Las empresas que emitan garantías financieras deben encontrarse bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, contar con clasificación de riesgo B o superior, y deben estar autorizadas para emitir garantías o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

4.4.2 La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).

4.4.3 Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía. Para fines de lo establecido en el artículo 61 de la Ley, la clasificación de riesgo B o superior.

4.4.4 Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en la sede digital de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en la Ley.

4.4.5 En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.

4.4.6 Además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse la sede digital de dicha entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).

4.5 CONSIDERACIONES PARA LOS DOCUMENTOS PÚBLICOS EXTENDIDOS EN EL EXTRANJERO

En el caso que los documentos requeridos para el perfeccionamiento del contrato incluyan documentos públicos extendidos en el exterior, que no les sea aplicable el Convenio de la Apostilla, se debe tener en cuenta que, de conformidad con lo previsto en el artículo 137 del Reglamento Consular del Perú, aprobado mediante Decreto Supremo N° 032-2023-RE, para que estos surtan efectos legales en el Perú deben estar legalizados por los funcionarios consulares peruanos competentes, cuyas firmas deben ser autenticadas posteriormente por el área competente del órgano de línea consular, además de cumplir con los requisitos adicionales que contemple la legislación peruana para su validez en el Perú.

4.6 DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento de selección no contemplados en las bases se rigen por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD CONTRATANTE DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO CON LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I
GENERALIDADES

1.1. BASE LEGAL

- Ley N° 32069, Ley General de Contrataciones Públicas.
- Decreto Supremo N° 009-2025-EF, Decreto Supremo que aprueba el Reglamento de la Ley General de Contrataciones Públicas.
- Ley de Presupuesto del Sector Público para el año fiscal N° 32185.
- Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal N° 321786
- Ley N° 27444, Ley del Procedimiento Administración General
- Ley N° 27785 Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
- Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado por el Decreto Supremo N° 043-2003-PCM.
- Código Civil.
- Directivas, pronunciamiento y opiniones emitidas por OSCE.
- Resoluciones Emitidas por el Tribunal de Contrataciones del Estado.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

1.2. ENTIDAD CONTRATANTE

Nombre	:	UNIVERSIDAD NACIONAL JOSE FAUSTINO SANCHEZ CARRION
RUC Nº	:	20172299742
Domicilio legal	:	Av. MERCEDES INDACOCHEA N° 600 – CUIDAD UNIVERSITARIA – HUACHO
Teléfono:	:	943734103
Correo electrónico:	:	procesos@unjfsc.edu.pe

1.3. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación para la Adquisición de Licencias Software Antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos para Asegurar la Continuidad Operativa de la Universidad, Así como la Protección de todas las Computadoras de la Universidad Nacional José Faustino Sánchez Carrión.

ÍTEM	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
1	Antivirus para servidores	16	unidad
2	Antivirus para computadoras	2088	unidad

1.4. CUANTÍA DE LA CONTRATACIÓN[2]

La cuantía de la contratación no se dará a conocer a los proveedores de conformidad con lo determinado en la estrategia de contratación y lo dispuesto en el numeral 53.4 del artículo 53 del Reglamento.

1.5. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado el Memorando N° 0141-2025-R-UNJFSC de fecha 11 de junio de 2025.

[2] El monto de la cuantía de la contratación indicado en esta sección de las bases no debe diferir del monto de la cuantía de la contratación consignado en la ficha del procedimiento de selección en el SEACE de la Pladicop. No obstante, de existir contradicción entre estos montos, primará el monto de la cuantía de la contratación indicado en las bases.

1.6. FUENTE DE FINANCIAMIENTO

La Fuente de financiamiento es Recursos Determinados.

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1 CRONOGRAMA DEL PROCEDIMIENTO DE SELECCIÓN

Según el cronograma de la ficha de selección de la convocatoria publicada en el SEACE de la Pladicop.

2.2 CONTENIDO DE LAS OFERTAS

La oferta contiene un índice de documentos[3] y la siguiente documentación:

2.2.1 Documentación de presentación obligatoria

2.1.1.1. Documentos para la admisión de la oferta:

Los evaluadores verifican la presentación de los documentos señalados en el presente acápite. De no cumplir con lo requerido, la oferta se considera no admitida. Los evaluadores no pueden incorporar documentos adicionales para la admisión de la oferta a los establecidos en este acápite.

a) Declaración jurada de datos del postor. (**Anexo Nº 1)**

b) Pacto de integridad (**Anexo N° 2)**

c) Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

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, estos documentos deben ser presentados por cada uno de los integrantes del consorcio que suscriban la promesa de consorcio, según corresponda.

Advertencia
De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa, las entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la entidad contratante es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[4] y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

d) Declaración jurada declarando que: (i) es responsable de la veracidad de los documentos e información de la oferta, y (ii) no se encuentra impedido para contratar con el Estado, de acuerdo con el artículo 33 de la Ley. **(Anexo Nº 3)**

e) Promesa de consorcio con firmas digitales, o en su defecto, firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el

[3] La omisión del índice no determina la no admisión de la oferta.
[4] Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma Nacional de Interoperabilidad – PIDE ingresar al siguiente enlace https://www.gob.pe/741-plataforma-nacional-de-interoperabilidad

domicilio común, el correo electrónico común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. (**Anexo Nº 4**)

f) Documentación que acredite la desafectación del impedimento, en caso el proveedor al registrarse como participante hubiera presentado la Declaración Jurada de Desafectación del Impedimento (**Anexo N° 5),** de conformidad con el numeral 39.4 del artículo 39 del Reglamento.

Advertencia
El requisito indicado en el literal f) únicamente se solicitará al proveedor que al registrarse hubiera presentado la Declaración Jurada de Desafectación del impedimento.

g) Oferta Económica **(Anexo N° 6).** En caso el requerimiento contenga prestaciones accesorias, la oferta económica individualiza los montos correspondientes a las prestaciones principales y las prestaciones accesorias.

2.1.1.2. Documentos para acreditar los requisitos de calificación
Incorporar en la oferta los documentos que acreditan los **"Requisitos de Calificación"** que se detallan en el numeral 3.5 del Capítulo III de la presente sección de las bases.

2.1.2. <u>Documentación de presentación facultativa</u>

2.1.2.1. Incorporar en la oferta los documentos que acreditan los "**Factores de Evaluación**" establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.

2.1.2.2. Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa **(Anexo Nº 16)**.

Advertencia
Los evaluadores no pueden exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".
<u>Importante para la entidad contratante</u>
Esta disposición solo debe ser incluida en el caso de procedimientos de selección cuya cuantía de la contratación sea igual o menor a cincuenta (50) UIT: *En caso el participante o postor opte por presentar recurso de apelación y por otorgar la garantía mediante depósito en cuenta bancaria, se debe realizar el abono en:* *<u>N° de Cuenta</u> : 00-321-024157* *<u>Banco</u> : Banco de la Nación* *<u>N° CCI</u>[5] : 018-321000321024157-00*

[5] En caso de transferencia interbancaria.

2.2. REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

a) Contrato de consorcio con firmas legalizadas ante notario de cada uno de los integrantes, de ser el caso.

b) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y nombre de la entidad bancaria en el exterior.

c) Copia de la vigencia del poder del representante legal del postor que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.

d) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

e) Autorización de notificaciones durante la ejecución del contrato al correo electrónico contemplado en el contrato (**Anexo Nº 9**).

f) Detalle de los precios unitarios del precio ofertado

g) Institución Arbitral elegida por el postor (**Anexo N° 10**).

h) Declaración Jurada actualizada de Desafectación de Impedimento **(Anexo N° 15)** y la documentación que acredite dicha desafectación.

Advertencia

- *De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la entidad contratante es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f) del presente numeral.*

- *La Institución Arbitral es elegida por el postor ganador de la buena pro de la lista de instituciones arbitrales que haya propuesto la entidad contratante en las bases del procedimiento de selección. Para dicho efecto, al remitir los documentos para la suscripción del contrato, el postor ganador de la buena pro comunica a la entidad contratante la Institución Arbitral elegida de la referida lista, caso contrario, acuerda con la entidad contratante una Institución Arbitral distinta. En caso de falta de acuerdo, la Institución Arbitral es elegida de la mencionada lista por la entidad contratante de manera definitiva. Las partes pueden establecer estipulaciones adicionales o modificatorias del convenio arbitral, en la medida que no contravengan las disposiciones de la normativa de contrataciones públicas y/o las disposiciones especiales contenidas en la normativa general de arbitraje.*

- *El requisito indicado en el literal m) únicamente se solicitará si el postor adjudicado hubiera presentado la Declaración Jurada de Desafectación del Impedimento en el procedimiento de selección.*

- *En caso el postor declare la inaplicabilidad del impedimento Tipo 4.D del inciso 4 del numeral 30.1 del artículo 30 de la Ley, referido a las personas inscritas en el Registro de Deudores Alimentarios Morosos del Poder Judicial (Redam) presenta la Declaración Jurada respectiva (Anexo N° 17)*

2.3. PERFECCIONAMIENTO DEL CONTRATO

La entidad contratante suscribe el contrato mediante firma digital, en caso de que el postor adjudicado con la buena pro cuente con certificado digital emitido por una entidad de certificación, de acuerdo con la normativa de la materia. Excepcionalmente, la entidad contratante con el debido sustento puede proceder a la firma del contrato mediante medios manuales.

El contrato firmado digitalmente se remite a la siguiente dirección electrónica: link https://facilita.gob.pe/t/4528, en caso de no contar con firma digital, la suscripción del contrato se realiza en la Oficina de Logística, sito en la Av. Mercedes Indacochea N° 600 Ciudad Universitaria

- Huacho.

2.4. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles.

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

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista en PAGO UNICO.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad contratante debe contar con la siguiente documentación:

- Documento de recepción y verificación del jefe de la Unidad de Almacén Central de la Universidad.
- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable del área usuaria la Oficina de Servicios Informáticos (OSI).
- Comprobante de pago.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, el contratista debe presentar la documentación restante en mesa de partes virtual en la siguiente dirección electrónica: link https://facilita.gob.pe/t/4528, sito en la Av. Mercedes Indacochea N° 600 Ciudad Universitaria - Huacho.

Advertencia
En caso se verifique que el proveedor tiene multas impagas que no se encuentren en procedimiento coactivo, se incorpora al contrato una cláusula de compromiso de pago de la multa, estableciéndose que durante la ejecución del contrato la entidad contratante retiene de forma prorrateada hasta el 10% del monto del contrato, para el pago o amortización de multas, conforme lo propuesto en la Cláusula Cuarta de la proforma de contrato.

CAPÍTULO III
REQUERIMIENTO

Advertencia
Al elaborar las bases, los evaluadores incluyen en esta sección el requerimiento que forma parte del expediente de contratación aprobado. El área usuaria es responsable de formular adecuadamente el requerimiento, en coordinación con la dependencia encargada de las contrataciones, de conformidad con el artículo 20 del Reglamento. El requerimiento debe elaborarse de acuerdo con el formato consignado en este capítulo y estar incluido en el cuadro multianual de necesidades.

3.1. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Garantizar la seguridad cibernética y la integridad de los sistemas de información utilizados en la institución. Estas licencias se adquieren con el propósito de proteger la información crítica, los datos académicos, la infraestructura de tecnología de la información y la privacidad de los usuarios, incluyendo estudiantes, profesores y personal administrativo. Al asegurar la protección de los servidores y computadoras, la universidad busca mantener un entorno digital seguro y confiable para el acceso a recursos académicos y administrativos, promoviendo así la continuidad de las operaciones y la calidad de la educación y la investigación que ofrece a la continuidad universitaria y la sociedad en general.

3.2. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Adquisición de Licencias Software Antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos para Asegurar la Continuidad Operativa de la Universidad, así como la Protección de todas las Computadoras de la Universidad Nacional José Faustino Sánchez Carrión.

3.3. CONDICIONES DE CONTRATACIÓN

a. Modalidad de pago

El contrato se rige por la modalidad de Suma Alzada, de conformidad con el artículo 130 del Reglamento.

b. Sistema de entrega

El contrato se rige por el sistema de entrega de Llave en mano

c. Plazo de entrega

Los bienes materia de la presente convocatoria se entregan en el plazo de 5 días y 5 ~~3~~ días para su instalación y puesta en funcionamiento, en concordancia con lo establecido en la estrategia de contratación.

d. Lugar de entrega de los bienes

Los bienes materia de la presente convocatoria se entregan en el Almacén Central de la Universidad sito en Av. Mercedes Indacochea N° 600 Huacho.

e. Penalidades

Penalidad por mora:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

h. Solución de controversias contractuales:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje.
Para el arbitraje, el postor ganador de la buena pro selecciona a uno de las siguientes Instituciones Arbitrales para administrar el arbitraje: Colegio de ingenieros del Perú, Cámara de

Comercio de Lima.

3.4 ESPECIFICACIONES TÉCNICAS

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

JEFATURA

ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN DE BIENES

1. **DENOMINACIÓN DE LA CONTRATACIÓN**

ADQUISICION DE LICENCIAS SOFTWARE ANTIVIRUS PARA LA PROTECCION DE LOS SISTEMAS DE INFORMACION DE LOS SERVIDORES DEL CENTRO DE DATOS PARA ASEGURAR LA CONTINUIDAD OPERATIVA DE LA UNIVERSIDAD, ASI COMO LA PROTECCION DE TODAS LAS COMPUTADORAS DE LA UNIVERSIDAD NACIONAL JOSE FAUSTINO SANCHEZ CARRION

2. **ÁREA USUARIA**

Oficina de Servicios Informáticos.

3. **OBJETIVO DE LA ADQUISICIÓN**

Adquirir licencias de antivirus por 365 días para la protección de los sistemas de información de los servidores del centro de datos para asegurar la continuidad operativa de la universidad, así como la protección de todas las computadoras de la universidad.

4. **FINALIDAD PÚBLICA**

Garantizar la seguridad cibernética y la integridad de los sistemas de información utilizados en la institución. Estas licencias se adquieren con el propósito de proteger la información crítica, los datos académicos, la infraestructura de tecnología de la información y la privacidad de los usuarios, incluyendo estudiantes, profesores y personal administrativo. Al asegurar la protección de los servidores y computadoras, la universidad busca mantener un entorno digital seguro y confiable para el acceso a recursos académicos y administrativos, promoviendo así la continuidad de las operaciones y la calidad de la educación y la investigación que ofrece a la continuidad universitaria y la sociedad en general.

5. **DESCRIPCIÓN DE LAS CARACTERÍSTICAS DEL BIEN (Especificaciones Técnicas)**

ÍTEM	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
1	Antivirus para servidores	16	unidad
2	Antivirus para computadoras	2088	unidad

ESPECIFICACINES TECNICAS	
ATRIBUTOS	**CARACTERISTICAS**
	Windows 11 Pro / Home / Enterprise / Education (32 bits / 64 bits) Windows 10 Home / Pro / Enterprise / Education (32 bits / 64 bits) Windows Server 2025 (Estándar / Datacenter / Essentials) Windows Server 2022 (Estándar / Datacenter / Essentials) Windows Server 2019 (Estándar / Datacenter / Essentials) Windows Server 2016 (Estándar / Datacenter) (64 bits) Windows Server 2012 R2 (Estándar / Datacenter) (64 bits) Windows MultiPoint Server 2012 (Estándar) (64 bits) Windows Server 2012 (Standard / Essentials / Foundation / Storage Server / Datacenter) (64 bits) Windows Server 2008 R2 (Web / Estándar / Empresa / Datacenter) (64 bits) Windows Server 2008 (Web / Estándar / Empresarial) (32 bits / 64 bits) / Datacenter (64 bits)

SISTEMAS OPERATIVOS	Fedora 30, 32, 38, 39 Linux Mint 19.3, 20, 21 Ubuntu 16.04, 18.04, 20.04, 22.04, 23.10 Debian 9, 10, 11, 12 CentOS 7.8, 8.2, Stream 8, Stream 9 RHEL 7.5, 7.8, 8.2, 8.6, 9.0, 9.2 Enterprise SUSE Linux 12 SP4, Enterprise Desktop 15, SUSE Linux Enterprise Server 15 SP5 Rocky Linux 8.4, 9.2 AlmaLinux 8.4, 9.2 Boss 6.0, 8.0, 9.0 Oracle Linux 7.1, 7.9, 8.1, 9.2 macOS Mac OS X 10.9, 10.10, 10.11 macOS 10.12, 10.13, 10.14, 10.15 macOS 11 (Big Sur) macOS 12 (Monterey) macOS 13 (Ventura) macOS 14 (Sonoma)
ACTUALIZACIONES	Las actualizaciones del fichero de firmas de virus y del motor de búsqueda deben de ser tanto manuales como automáticas (programadas) en servidores y estaciones de trabajo. La solución debe de contar con la capacidad de obtenerlas directamente desde Internet o desde un servidor local de actualizaciones para entornos restringidos con políticas de seguridad estrictas. La solución debe de permitir la creación y administración de repositorios distribuidos y programados, optimizando la distribución de las actualizaciones en infraestructuras empresariales de múltiples nodos. Además, la solución debería de garantizar alta disponibilidad y redundancia mediante replicación automática y sincronización diferencial. Las actualizaciones deben de contar con la opción de realizarse en modalidad completa o incremental. La solución debería de asegurar un consumo eficiente del ancho de banda y reducir la latencia en redes empresariales mediante algoritmos de compresión y deduplicación. El motor de detección de amenazas debe de estar basado en inteligencia artificial (IA), aprendizaje profundo (Deep Learning) y análisis de comportamiento (Behavioral Analysis). La solución debe de permitir la identificación proactiva de amenazas avanzadas como malware polimórfico, fileless malware, ataques de día cero y amenazas persistentes avanzadas (APT). Las actualizaciones deben de realizarse con una frecuencia mínima de una vez por hora en los siguientes componentes clave: • **Fichero de firmas de virus:** La solución debe de incluir una base de datos centralizada con firmas de amenazas conocidas, incluyendo hash de archivos maliciosos y patrones de comportamiento. • **Motor heurístico y análisis de código estático:** La solución debería de permitir la identificación de variantes desconocidas basadas en modelos predictivos de IA. • **Base de datos de inteligencia de amenazas (Threat Intelligence):** La solución debe de integrarse con plataformas globales de ciberseguridad para la correlación de amenazas en tiempo real. • **Módulos de detección avanzada:** La solución debe de ofrecer protección contra amenazas avanzadas a nivel de endpoints con capacidades de telemetría y análisis forense automatizado. • **Sistema de prevención y respuesta ante incidentes (Incident Response & SOAR):** La solución debería de contar con la capacidad para generar alertas y mitigar amenazas de forma autónoma. El motor de análisis debe de incluir técnicas avanzadas como Sandboxing y Deception Technology. La solución debería de permitir la ejecución de archivos sospechosos en entornos virtualizados y generar alertas cuando se detecten intentos de evasión de seguridad. Debe de contar con un modelo Zero Trust aplicado a la seguridad endpoint. La solución debe de garantizar que todas las aplicaciones, procesos y conexiones sean verificadas antes de ser ejecutadas en el sistema. Las actualizaciones y detección de amenazas deben de estar reforzadas con mecanismos de seguridad criptográfica, incluyendo: • **Integridad mediante firmas digitales (SHA-256 o superior):** La solución debe de evitar alteraciones en los paquetes de actualización. • **Canales de comunicación cifrados (TLS 1.3, AES-256):** La solución debería de garantizar la distribución segura de las actualizaciones.

	• **Autenticación de doble factor (2FA) y gestión de accesos con privilegios mínimos (PAM):** La solución debe de prevenir manipulaciones no autorizadas. La solución debe de permitir la reversión (Rollback) de actualizaciones de firmas y motor de búsqueda, con la capacidad de restaurar automáticamente versiones previas en caso de fallos, incompatibilidades o falsos positivos.
PROTECCIÓN PROACTIVA	La solución debe de contar con detección proactiva y protección avanzada contra amenazas. La solución debe de contar con un motor de detección basado en inteligencia artificial (AI-driven threat detection), machine learning (ML) y análisis heurístico avanzado, permitiendo la identificación de malware en múltiples fases del ciclo de vida de la amenaza: • **Pre-execution (antes de la ejecución):** La solución debe de contar con emulación dinámica del código, técnicas de análisis estático, detección sin firmas (signatureless detection) y validación con threat intelligence en la nube. • **On-execution (durante la ejecución):** La solución debe de realizar behavioral analysis, detección de procesos maliciosos en tiempo real y modelo de Zero Trust, garantizando que ninguna aplicación o proceso no autorizado se ejecute sin verificación previa. • **Post-execution (respuesta y contención):** La solución debe de implementar Extended Detection and Response con capacidades de threat hunting, permitiendo correlacionar eventos, automatizar respuestas y generar análisis forenses de seguridad. La solución debe de implementar manejo de DNS virtual con AI-driven Secure DNS, asegurando conexiones cifradas, evitando DNS hijacking, MITM attacks, DNS spoofing y cache poisoning. El módulo de protección bancaria de la solución debe de crear un entorno seguro con navegación aislada (Isolated Secure Browser), ejecución en contenedores seguros (Containerized Execution) y validación de sitios con Blockchain-based Integrity, minimizando la exposición a ataques de fraude financiero. La solución debe de emplear Behavioral Biometrics y AI-powered User Authentication, analizando patrones de navegación y comportamiento del usuario para detectar anomalías en sesiones de banca en línea. La solución debe de incluir un motor de análisis de comportamiento con Deep Learning y Threat Graph AI, permitiendo identificar técnicas avanzadas de evasión como: • Malware polimórfico y metamórfico • Code injection y memory injection attacks • Fileless malware (ataques sin archivos ejecutables) • Process hollowing, DLL hijacking y API hooking • Integración con Threat Intelligence Feeds en tiempo real (STIX/TAXII) La solución debe de contar con la incorporación de un Next-Generation IDS/IPS (NG-IDS/IPS) con detección basada en AI y correlación de eventos de seguridad con UEBA (User and Entity Behavior Analytics). La solución debe de implementar AI-powered Network Traffic Analysis (NTA) para detectar anomalías en patrones de tráfico y Deep Packet Inspection (DPI) con TLS 1.3 decryption, permitiendo inspección de tráfico cifrado. La solución debe de contar con auto-remediación y segmentación de red dinámica, integrando mecanismos de microsegmentation y Zero Trust Network Access (ZTNA) para evitar movimientos laterales de atacantes dentro de la infraestructura empresarial. El módulo de Backup and Restore de la solución debe de contar con: • Cifrado quantum-resistant de al menos 4096 bits para garantizar resistencia ante ataques criptográficos futuros. • Blockchain-based Integrity Verification, asegurando que los archivos respaldados no sean alterados ni manipulados por actores malintencionados. • Air-gapped Backup Support, permitiendo almacenamiento desconectado y protegido contra ataques como ransomware y wiper malware. • File Entropy Analysis, permitiendo detectar archivos alterados o con riesgo de corrupción. La solución debe de implementar Secure Boot y Runtime Integrity Verification, garantizando que el sistema operativo y los archivos críticos no sean modificados por malware. La solución debe de contar con un modelo Zero Trust aplicado al endpoint, asegurando que cada proceso, aplicación y servicio sea verificado antes de ser ejecutado. La solución debe de implementar AI-powered Patch Management System, permitiendo la detección y remediación automática de vulnerabilidades en el sistema operativo y aplicaciones. La solución debe de contar con mecanismos de antimanipulación avanzada (Self-Defense Mechanisms), evitando que el sistema de seguridad sea deshabilitado por malware.
CONTROL Y PRODUCTIVIDAD EN LA RED	La solución debe de contar con un módulo de control de aplicaciones y gestión de software no autorizado. • La solución debe de contar con un sistema avanzado de control de aplicaciones (Next-Gen Application Control) que permita la supervisión, restricción y bloqueo dinámico de software en ejecución, alineado con los principios de Zero Trust Application Execution (ZTAE). • La solución debe de operar mediante listas blancas y negras (Application Whitelisting & Blacklisting)

	administradas por IA, permitiendo la detección en tiempo real de aplicaciones sospechosas con base en su hash, comportamiento en memoria y origen del ejecutable. • La solución debe de contar con capacidad de desinstalación remota de aplicaciones no autorizadas, incluyendo herramientas P2P, software de control remoto sospechoso y aplicaciones Shadow IT desde la consola central. • La solución debe de ofrecer protección contra ataques de escalamiento de privilegios (Privilege Escalation Protection), asegurando que las aplicaciones restringidas no puedan obtener permisos administrativos para ejecutarse de manera no autorizada. • La solución debe de realizar análisis de comportamiento en ejecución (Behavioral AI-Based Application Monitoring) para detectar ataques mediante Process Hollowing, DLL Hijacking y API Hooking. • La solución debe de integrarse con AI-Powered Threat Intelligence Feeds (STIX/TAXII) para actualizar dinámicamente las listas de software malicioso en base a inteligencia global de amenazas. • La solución debe de contar con bloqueo de ejecución de aplicaciones modificadas (Tamper Detection), impidiendo la ejecución de binarios alterados o parcheados por malware en memoria. • La solución debe de restringir software de mensajería instantánea y redes sociales (MSN, Yahoo Messenger, Google Talk, Telegram, WhatsApp, Discord, Signal, etc.). • La solución debe de bloquear aplicaciones de Voz sobre IP (VoIP) (MSN, Skype, Google Talk, Zoom, Webex, etc.). • La solución debe de impedir la ejecución de software Peer-to-Peer (P2P) (Kazaa, Ares, BitTorrent, uTorrent, eMule, etc.). • La solución debe de restringir juegos en red y Stand-Alone en entornos corporativos. • La solución debe de bloquear barras de herramientas y plugins no autorizados que puedan contener spyware o malware. • La solución debe de evitar el uso de herramientas de control remoto (RATs), como LogMeIn, AnyDesk, TeamViewer, VNC y Netcat. • La solución debe de identificar y bloquear aplicaciones Shadow IT y ejecutables no firmados, bloqueando cualquier software sin validación criptográfica previa. • La solución debe de contar con un sistema de gestión de vulnerabilidades (Vulnerability & Exposure Management), capaz de: • Escanear, identificar y clasificar vulnerabilidades en software y sistemas operativos. • Aplicar parches de seguridad de forma automatizada mediante un sistema de Patch Management basado en IA. • Detectar configuraciones inseguras (Misconfiguration Detection) y generar alertas para su corrección. • Evitar la explotación de vulnerabilidades Zero-Day con tecnología de AI-Powered Exploit Prevention. • La solución debe de integrarse con Threat Intelligence Feeds en tiempo real para actualizar bases de datos de vulnerabilidades explotadas activamente (CVE Exploit Monitoring). • La solución debe de contar con prevención contra ataques a firmware y BIOS (Firmware Integrity Protection) mediante Secure Boot y Runtime Code Integrity Verification. • La solución debe de aplicar el modelo Zero Trust a la detección de vulnerabilidades, impidiendo que sistemas desactualizados se conecten a la red sin validación previa. • La solución debe de contar con un sistema avanzado de monitoreo de actividad de archivos (Next-Gen File Activity Monitoring - NG-FAM), capaz de: • Rastrear en tiempo real la actividad de archivos críticos en servidores y endpoints. • Generar alertas cuando se detecte acceso, copia, renombrado, modificación o eliminación de archivos confidenciales. • Aplicar cifrado automático y control de acceso basado en contexto (Context-Aware Access Control - CAAC) para evitar filtraciones de datos. • Prevenir el uso no autorizado de medios extraíbles (USB, SD, almacenamiento externo), asegurando cifrado automático de archivos sensibles. • La solución debe de contar con análisis forense de incidentes de seguridad (Forensic Data Analysis & Insider Threat Detection), generando registros detallados de actividad sospechosa. La solución debe de contar con un sistema de detección y prevención de intrusos (Next-Gen IDS/IPS) con capacidades de: • AI-Powered Network Traffic Analysis (NTA) para detectar anomalías en tráfico cifrado. • Deep Packet Inspection (DPI) con TLS 1.3 Decryption, inspeccionando paquetes sospechosos en tiempo real.

	Segmentación dinámica de red (Adaptive Microsegmentation), impidiendo movimientos laterales de atacantes dentro de la red. Protección contra ataques de exfiltración de datos (Data Exfiltration Protection - DEP). • La solución debe de contar con prevención de ataques fileless y técnicas de evasión avanzada (Evasion-Resistant Security Engine), bloqueando: • Living Off The Land Attacks (LOTL). • Process Injection y Reflective DLL Loading. o Malware en memoria sin archivos ejecutables (Fileless Malware Protection). • Ataques basados en PowerShell, WMI y macros maliciosas.
CONTROL DE DISPOSITIVOS	La solución debe de contar con un control avanzado de dispositivos y restricción de acceso. • La solución debe de permitir bloquear el acceso a dispositivos físicos y virtuales mediante reglas predefinidas y políticas de seguridad centralizadas, asegurando un modelo Zero Trust de control de dispositivos en la red corporativa. • La solución debe de ser capaz de agregar y gestionar dispositivos con identificación granular mediante Class ID, Hardware ID (HW ID) y Device Instance ID, permitiendo políticas de restricción avanzadas y evitando la manipulación de identificadores de hardware. • La solución debe de ofrecer un motor de control de dispositivos basado en inteligencia artificial (AI-Driven Device Control), permitiendo: • La solución debe de permitir detección y bloqueo de dispositivos maliciosos o no autorizados en tiempo real. • La solución debe de automatizar respuestas a intentos de conexión de dispositivos sospechosos. • La solución debe de generar alertas sobre intentos de acceso no autorizado o intentos de falsificación de identificadores de hardware. • La solución debe de contar con una política de restricción basada en el contexto (Context-Aware Device Policy), asegurando que ciertos dispositivos solo puedan ser utilizados en ubicaciones específicas o por usuarios autorizados. • La solución debe de generar reportes detallados sobre el uso de dispositivos, registros de acceso y auditoría de intentos de conexión fallidos. La solución debe de permitir la restricción, monitoreo y bloqueo de acceso a los siguientes dispositivos: • La solución debe de evitar modificaciones en discos de almacenamiento locales sin permisos específicos. • La solución debe de gestionar almacenamiento removible (USB, discos duros externos, SD cards) con capacidad de aplicar cifrado automático para unidades permitidas. • La solución debe de asegurar que solo impresoras locales y de red aprobadas puedan procesar documentos. • La solución debe de restringir lectura/escritura en CD/DVD y detectar medios maliciosos. • La solución debe de impedir el uso de unidades de diskette con vulnerabilidades conocidas. • La solución debe de garantizar que los módems no generen conexiones externas no autorizadas. • La solución debe de limitar el acceso a dispositivos de cinta para almacenamiento de gran capacidad. • La solución debe de controlar dispositivos multifuncionales (impresoras, escáneres, copiadoras con almacenamiento integrado). • La solución debe de permitir el acceso solo a lectores de Smart Cards y tokens USB certificados. • La solución debe de restringir la sincronización de dispositivos como smartphones, PDAs y tablets para evitar intercambio de archivos no autorizado. • La solución debe de bloquear dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.). • La solución debe de aplicar políticas de acceso a redes inalámbricas corporativas y bloquear Wi-Fi adapters desconocidos. • La solución debe de impedir conexiones no autorizadas mediante adaptadores de red externos (Ethernet, USB to LAN). • La solución debe de bloquear la transferencia de datos no autorizada en dispositivos MP3 o teléfonos inteligentes. • La solución debe de restringir el intercambio de archivos vía Bluetooth y evitar ataques de sniffing o Bluejacking. • La solución debe de aplicar un modelo Zero Trust Device Access donde ningún dispositivo pueda conectarse sin validación previa.

	• La solución debe de contar con USB Threat Protection, implementando escaneo en tiempo real de dispositivos USB para detectar y neutralizar malware antes de que pueda ejecutarse. • La solución debe de ofrecer AI-Powered Device Behavior Analytics para analizar el uso de dispositivos y detectar comportamientos anómalos e intentos de acceso sospechosos. • La solución debe de garantizar Secure Removable Storage Encryption, cifrando unidades USB y otros dispositivos de almacenamiento removible para la protección de datos. • La solución debe de restringir conexiones a redes y dispositivos inalámbricos no aprobados con Bluetooth and Wi-Fi Intrusion Prevention para prevenir ataques de proximidad. • La solución debe de permitir la creación de listas blancas y negras de dispositivos permitidos y bloqueados según su identificador único de hardware con Device Whitelisting & Blacklisting. • La solución debe de contar con un comando de bloqueo remoto y desactivación para inutilizar dispositivos en caso de intento de acceso no autorizado o actividad sospechosa. • La solución debe de generar registros detallados de intentos de acceso, bloqueos aplicados y políticas activas sobre dispositivos con Forensic Logging & Audit Trails.
INSTALACIÓN	La solución debe de permitir instalación remota, gestión centralizada y descubrimiento automático de equipos. • La solución debe de permitir instalación remota desde una herramienta del propio fabricante, asegurando un despliegue automatizado, seguro y escalable en todos los equipos dentro de la infraestructura de TI. • La solución debe de realizar la instalación mediante el envío de un agente ligero con todos los módulos de protección preconfigurados, garantizando que cada endpoint reciba la configuración de seguridad adecuada según su nivel de acceso y tipo de usuario. • La solución debe de ser compatible con modelos de despliegue Zero Trust, asegurando que solo dispositivos autenticados y autorizados puedan instalar y ejecutar el software de protección. • La solución debe de contar con la capacidad de detectar y reconocer máquinas virtuales en plataformas: o VMware ESXi, Workstation y Fusion. o Microsoft Hyper-V (incluyendo entornos en Azure). o Virtual PC, Parallels Desktop, Oracle VirtualBox. o Xen Server y KVM. o Soporte para contenedores Docker/Kubernetes. • La solución debe de detectar entornos de ejecución aislados o sandboxing, evitando la ejecución del agente en entornos de análisis maliciosos que busquen evadir detecciones. • La solución debe de contar con la capacidad de analizar la estructura de Active Directory (AD) para descubrir y mapear equipos en la red, facilitando la implementación en entornos corporativos complejos. • La solución debe de sincronizar automáticamente con Organizational Units (OU) de Active Directory, asegurando que cada equipo reciba las políticas de seguridad adecuadas. • La solución debe de ser compatible con Microsoft Entra ID (Azure Active Directory), permitiendo gestión híbrida de dispositivos locales y en la nube. • La solución debe de implementar Network Access Control (NAC) para validar que los dispositivos cumplen con los requisitos de seguridad antes de permitir la instalación. La solución debe de ofrecer múltiples opciones para garantizar flexibilidad y seguridad en la implementación: • La solución debe de permitir instalación desde la consola de administración, permitiendo despliegue masivo con políticas predefinidas. • La solución debe de sincronizarse con Active Directory para despliegue automatizado en entornos Windows y Azure AD. • La solución debe de permitir instalación mediante recurso UNC (Universal Naming Convention), facilitando el despliegue en redes corporativas sin inter • vención del usuario. • La solución debe de permitir distribución mediante CD/DVD o USB cifrados, asegurando integridad en entornos offline o altamente restringidos. • La solución debe de permitir instalación desde una página web con autenticación segura (usuario y clave), permitiendo despliegue en equipos fuera de la LAN mediante VPN. • La solución debe de ser compatible con herramientas de gestión de despliegue como SCCM, Ansible, Puppet, Chef y Microsoft Intune. • La solución debe de permitir la gestión centralizada de equipos remotos (clientes roaming) sin necesidad de exponer la consola en una zona desmilitarizada (DMZ) o depender de configuraciones de seguridad vulnerables. • La solución debe de contar con un mecanismo de actualización de estaciones de trabajo fuera de la red corporativa, asegurando que los endpoints mantengan las últimas firmas de seguridad sin comprometer la integridad de la infraestructura de TI. • La solución debe de implementar un modelo de actualización seguro basado en AI-Powered Threat Intelligence, evitando conexiones con servidores de actualización comprometidos o suplantados.

	• La solución debe de integrarse con Cloud-Based Secure Gateway, permitiendo que los clientes roaming accedan a actualizaciones a través de servidores de actualización distribuidos con comunicación cifrada y validación criptográfica. • La solución debe de ofrecer un modo de actualización P2P (Peer-to-Peer) para estaciones de trabajo dentro de la misma red, optimizando el consumo de ancho de banda en sucursales remotas o redes corporativas descentralizadas. • La solución debe de contar con instalación con validación de integridad criptográfica (SHA-256 o superior), asegurando que el agente no haya sido alterado antes de su ejecución. • La solución debe de ofrecer protección contra rootkits y malware persistente, evitando que software malicioso interfiera en la instalación del antivirus. • La solución debe de realizar un escaneo preinstalación (Pre-Deployment Security Check), asegurando que el equipo no esté comprometido antes de la implementación del software. • La solución debe de contar con antimanipulación avanzada (Self-Defense Mechanisms), impidiendo que malware modifique, detenga o elimine los módulos de seguridad. • La solución debe de proteger contra ejecución en entornos sandbox o máquinas virtuales fraudulentas, evitando que atacantes analicen el comportamiento del agente. • La solución debe de generar logs forenses y auditoría en tiempo real, permitiendo rastrear intentos de instalación no autorizados o fallos de seguridad en la implementación.
CONSOLA DE ADMINISTRACION	La solución debe de contar con una consola de administración centralizada on-premise. • La solución debe de ser una consola de administración on-premise que opere en la red mediante un servidor dedicado (localhost) con configuración segura de IPs y puertos de comunicación, asegurando integridad y autenticidad mediante TLS 1.3 y AES-256 para cifrado. • La solución debe de permitir gestión centralizada de antivirus, firewall, protección de endpoints y módulos de seguridad adicionales. • La solución debe de ofrecer comunicación bidireccional basada en eventos, reduciendo tráfico innecesario en la red y mejorando la eficiencia en la entrega de actualizaciones y reportes de incidentes. • La solución debe de contar con capacidad de escalabilidad para administrar redes corporativas complejas con más de 2700 dispositivos conectados, con balanceo de carga inteligente para optimizar el rendimiento. • La solución debe de implementar Zero Trust Security Model, asegurando que ningún dispositivo se conecte sin autenticación previa y validación de cumplimiento de políticas de seguridad. • La solución debe de permitir la administración simultánea de estaciones y servidores en Windows, Linux y Mac, con despliegue de políticas de seguridad y detección de amenazas en todos los sistemas operativos compatibles. • La solución debe de sincronizar automáticamente con Active Directory (AD) y Microsoft Entra ID (Azure AD) para descubrimiento de equipos y asignación de políticas de seguridad. • La solución debe de ser compatible con entornos virtualizados, incluyendo: • VMware ESXi, Workstation y Fusion. • Microsoft Hyper-V. • Oracle VirtualBox, Xen Server y KVM. • Soporte para Docker y Kubernetes Security Policies. • La solución debe de integrarse con Network Access Control (NAC) para validar dispositivos antes de permitir su sincronización con la consola. • La solución debe de contar con capacidad de descubrimiento automático de equipos en red usando múltiples métodos: o TCP/IP Scanning. o Active Directory Sync. o ARP Scanning. o SNMP Monitoring. • La solución debe de generar paquetes de instalación personalizados, incluyendo la licencia y configuración del producto, con opciones de caducidad de 30/60/90 días para seguridad. • La solución debe de permitir instalación masiva y automatizada desde la Consola de Administración, permitiendo: • Despliegue por GPO a través de Active Directory. • Instalación mediante recurso UNC (Universal Naming Convention). • Instalación desde página web con autenticación segura para equipos fuera de la LAN. • Distribución vía correo electrónico mediante archivos ejecutables preconfigurados. • La solución debe de ser compatible con herramientas de despliegue como SCCM, Ansible, Puppet, Chef y Microsoft Intune. • La solución debe de proteger los procesos y servicios del antivirus mediante tecnologías de Self-Defense, evitando su desactivación o manipulación por malware. • La solución debe de realizar un escaneo Pre-Deployment para verificar que los equipos no estén comprometidos antes de la instalación del antivirus. • La solución debe de garantizar frecuencia de actualización de firmas de virus en tiempo real, asegurando detección inmediata de amenazas emergentes.

	• La solución debe de contar con una política de actualización adaptable para redes con conexiones limitadas, permitiendo: • Limitación de ancho de banda para actualizaciones en equipos con conexión lenta. • Elección de uno o varios equipos como repositorios de actualizaciones de firmas o software. • La solución debe de ser compatible con repositorios descentralizados, permitiendo la optimización del tráfico en la red sin requerir un servidor de administración adicional. • La solución debe de permitir: o Monitoreo en tiempo real de estaciones y servidores para detectar amenazas, infecciones y comportamientos sospechosos. • Control granular de actualizaciones y estado de seguridad de cada equipo conectado a la red. • Detección de equipos no protegidos o que no cumplen con las políticas de seguridad. • Capacidad de realizar escaneos simultáneos, programados o manuales, a nivel de red o por grupos de dispositivos. • Implementación de Response Automation (SOAR), permitiendo respuestas automáticas a amenazas críticas. • La solución debe de ofrecer detección y limpieza remota de amenazas, incluyendo: o Adware. o Aplicaciones potencialmente peligrosas (PUA). o Virus, troyanos, gusanos, spyware y ransomware. • La solución debe de proporcionar protección contra ataques basados en exploits y amenazas persistentes avanzadas (APT Protection). • La solución debe de contar con un módulo de control de contenido web, permitiendo bloquear o restringir: • Redes sociales. • Contenido violento o para adultos. • Streaming de video y plataformas de entretenimiento. • Sitios que ejecuten Flash, Silverlight, Java y ActiveX sin certificación. • La solución debe de incluir un sistema de firewall centralizado con IPS/IDS para prevenir ataques de red y amenazas de exfiltración de datos. • La solución debe de generar reportes detallados sobre el estado de seguridad de la infraestructura, incluyendo: • Antivirus instalado y en ejecución. • Última actualización y escaneo de cada equipo. • Cantidad y tipo de amenazas detectadas. • Estado de cumplimiento de políticas de seguridad. • Usuarios atacados, usuarios infectados y reportes de violaciones de seguridad. • La solución debe de permitir generación y exportación de reportes en formatos XML, CSV, PDF y HTML. • La solución debe de generar alertas y notificaciones en tiempo real vía correo electrónico y web en caso de ataques o eventos críticos. • La solución debe de contar con capacidad de generar eventos SNMP para monitoreo en soluciones SIEM (Security Information and Event Management). • La solución debe de permitir creación de usuarios administradores con privilegios diferenciados (Administración total o solo consulta). • La solución debe de forzar políticas de seguridad en equipos que hayan sido modificados localmente. • La solución debe de implementar AI-driven Anomaly Detection, permitiendo identificar comportamientos sospechosos en dispositivos o usuarios. • La solución debe de contar con capacidad de monitorear sesiones activas, direcciones IP, aplicaciones instaladas y estado de actualización de software en cada endpoint. • La solución debe de ser compatible con navegadores Mozilla Firefox, Microsoft Edge, Google Chrome, Opera y Safari. • La solución debe de contar con una vista avanzada para establecer políticas de seguridad personalizadas por grupo o por usuario.
DEFENSA INTEGRADA CONTRA MALWARE PROTECCIÓN CONTRA: VIRUS, TROYANOS, MACRO VIRUS, VIRUS GUSANO, SPYWARE, ADWARE. VIRUS EN	La solución debe de contar con una solución integrada de seguridad para estaciones y servidores. • La solución debe de ser integrada y contar con un único instalador multiplataforma que proporcione protección avanzada contra amenazas cibernéticas, incluyendo: • La solución debe de detectar virus, malware polimórfico y fileless malware. • La solución debe de proteger contra spyware, adware y ataques basados en phishing. • La solución debe de analizar comportamientos sospechosos mediante análisis heurístico y machine learning.

ARCHIVOS COMPRIMIDOS Y PUAS (APLICACIONES POTENCIALMENTE PELIGROSAS).	• La solución debe de defender contra ataques dirigidos y amenazas persistentes avanzadas (APT). • La solución debe de incluir protección contra hackers mediante firewall con reglas personalizables y segmentación de tráfico por servicios y protocolos de red. • La solución debe de detectar y bloquear aplicaciones potencialmente peligrosas (PUA). • La solución debe de contar con capacidad de protección en todos los protocolos de la red, asegurando escaneo profundo de tráfico HTTP, HTTPS, FTP, SMB, POP3, IMAP, SMTP y DNS. • La solución debe de utilizar inteligencia artificial para detección de amenazas en tiempo real, con actualización dinámica basada en Threat Intelligence Feeds y análisis de comportamiento (UEBA). • La solución debe de verificar únicamente archivos nuevos o modificados, optimizando el uso de recursos en sistemas críticos. • La solución debe de contar con respaldo automático de archivos críticos, con cifrado AES-256 para proteger información de ofimática y sistema operativo contra ransomware. • La solución debe de permitir emulación de archivos mediante heurística avanzada (sandboxing), ejecutando archivos sospechosos en entornos virtualizados para analizar su comportamiento antes de permitir su ejecución en el sistema. • La solución debe de ofrecer pausado programable de la protección, permitiendo su desactivación temporal con políticas administradas desde la consola central. • La solución debe de incluir prevención contra exploits (Exploit Prevention), protegiendo contra códigos maliciosos que explotan vulnerabilidades en aplicaciones populares como Adobe Reader, Java, Internet Explorer y navegadores modernos. • La solución debe de ser compatible con políticas de seguridad de Cisco NAC, asegurando control de acceso a la red basado en el cumplimiento de normativas corporativas. • La solución debe de incluir firewall avanzado del mismo fabricante, con administración centralizada de reglas y segmentación de tráfico de red. • La solución debe de bloquear y autorizar aplicaciones y puertos específicos tanto local como centralizadamente. • La solución debe de operar en "modo oculto", asegurando que el endpoint no sea detectado en exploraciones de red maliciosas. • La solución debe de generar alertas y registros en tiempo real sobre intentos de acceso no autorizado. • La solución debe de contar con un módulo especializado para control de contenido, con restricción granular para grupos específicos de usuarios o dispositivos. • La solución debe de permitir filtrado de acceso a sitios web y aplicaciones con reglas diferenciales para: • Redes sociales. • Contenido violento o para adultos. • Streaming de video y plataformas de entretenimiento. • Descarga de archivos ejecutables y aplicaciones P2P. • Ejecutables de Java, ActiveX, Flash y Silverlight provenientes de fuentes no confiables. • La solución debe de contar con versión para Linux con módulo de escaneo de alto rendimiento, asegurando estabilidad y eficacia. • La solución debe de ofrecer capacidad de escaneo en acceso, bajo demanda y programado en unidades locales, extraíbles y compartidas como NFS, Samba y otros sistemas de archivos. • La solución debe de integrarse con la consola central de administración, permitiendo configuración remota y gestión centralizada. • La solución debe de permitir configuración mediante línea de comandos y una interfaz web local, asegurando compatibilidad con entornos empresariales. • La solución debe de contar con certificación RedHat Ready o Novell SUSE Linux para compatibilidad con sistemas empresariales de alto rendimiento. • La solución debe de incluir un módulo de detección y prevención de intrusiones (IDS/IPS), capaz de identificar y mitigar ataques de escaneo de puertos ("Port Scan"). • La solución debe de permitir análisis de tráfico en tiempo real con algoritmos de Machine Learning para detectar tráfico malicioso en la red. • La solución debe de ofrecer segmentación dinámica del tráfico y reglas personalizadas para bloquear intentos de explotación de vulnerabilidades. • La solución debe de contar con filtrado avanzado de amenazas mediante sandbox configurable, ejecutando archivos sospechosos en entornos virtualizados antes de permitir su ejecución real en el endpoint. • La solución debe de ofrecer protección proactiva contra exploits, detectando intentos de ejecución de código malicioso en aplicaciones vulnerables. • La solución debe de permitir generación de "listas blancas" de software confiable basado en firmas digitales, asegurando que solo aplicaciones verificadas puedan ejecutarse.

	• La solución debe de incluir un módulo de cuarentena administrado por el usuario final, permitiendo controlar y autorizar la ejecución de aplicaciones bloqueadas. • La solución debe de generar copias de seguridad antes de cualquier intento de desinfección o eliminación de archivos, asegurando recuperación en caso de error. • La solución debe de permitir notificaciones en tiempo real a la consola central sobre detección de virus, spyware, adware, aplicaciones no deseadas, intentos de intrusión y cambios en la configuración del cliente antivirus/firewall. • La solución debe de contar con capacidad de actualizarse desde múltiples repositorios asignados en la consola web del fabricante simultáneamente, asegurando redundancia y máxima protección. • La solución debe de permitir distribución de actualizaciones en entornos con ancho de banda limitado, con políticas adaptativas y capacidad de establecer servidores de actualización locales.
ACTUALIZADOR DE SOFTWARE Y GESTIÓN DE ACTIVOS	La solución debe de contar con gestión automática de parches (Patch Management). • La solución debe de ser capaz de identificar, clasificar y priorizar actualizaciones de seguridad en aplicaciones y sistemas operativos según su nivel de criticidad y riesgo de explotación. • La solución debe de integrarse con bases de datos de vulnerabilidades CVE (Common Vulnerabilities and Exposures) para correlación de amenazas en tiempo real, permitiendo tomar acciones proactivas antes de que las vulnerabilidades sean explotadas. • La solución debe de contar con AI-Driven Patch Prioritization, utilizando Machine Learning para analizar el impacto de cada parche antes de su implementación y mitigar interrupciones operativas. • La solución debe de ser capaz de actualizar aplicaciones empresariales y software de terceros, incluyendo: • La solución debe de gestionar Microsoft Windows Updates (WSUS). • La solución debe de ofrecer Linux Patch Management con compatibilidad Red Hat, Debian, Ubuntu, CentOS y SUSE. • La solución debe de administrar macOS Patch Management para actualizaciones de seguridad en entornos Apple. • La solución debe de gestionar software de productividad como Microsoft Office, Adobe Reader, Google Chrome, Mozilla Firefox, Java y más. • La solución debe de permitir gestión centralizada de parches desde la consola de administración, permitiendo: • La solución debe de realizar despliegue automático o programado de actualizaciones en endpoints y servidores. • La solución debe de validar parches antes de su aplicación para evitar incompatibilidades. • La solución debe de permitir rollback de parches en caso de fallas, asegurando estabilidad del sistema. • La solución debe de establecer políticas de actualización diferenciadas por grupos de dispositivos y usuarios. • La solución debe de optimizar la distribución inteligente de parches minimizando el consumo de ancho de banda. • La solución debe de proporcionar parcheo proactivo para entornos desconectados, asegurando que estaciones de trabajo fuera de la red corporativa también reciban actualizaciones críticas. • La solución debe de priorizar actualizaciones basadas en análisis de comportamiento, permitiendo bloquear exploits activos antes de la aplicación del parche oficial. • La solución debe de contar con un módulo de supervisión de configuraciones de hardware y software en cada terminal, permitiendo a los administradores: • La solución debe de detectar cambios en el hardware en tiempo real (reemplazo de discos, aumento de memoria, cambios de tarjeta de red, etc.). • La solución debe de monitorizar la instalación, desinstalación y modificaciones de software en cada endpoint. • La solución debe de detectar alteraciones en archivos de configuración del sistema, claves de registro y servicios críticos. • La solución debe de bloquear la ejecución de software no autorizado mediante Whitelisting & Blacklisting de aplicaciones. • La solución debe de generar alertas automáticas ante configuraciones de hardware sospechosas que puedan estar relacionadas con ataques físicos o intentos de manipulación. • La solución debe de proteger contra rootkits y malware persistente, asegurando la integridad de los sistemas mediante Secure Boot y Runtime Integrity Verification. • La solución debe de integrarse con herramientas SIEM (Security Information and Event Management) mediante logs de seguridad y eventos SNMP para auditoría forense. • La solución debe de ser compatible con Network Access Control (NAC) para evitar que dispositivos con configuraciones no autorizadas accedan a la red corporativa.

	• La solución debe de garantizar cifrado de logs de monitoreo en AES-256 y almacenamiento seguro en servidores centralizados, asegurando la integridad y no alteración de los registros de seguridad. • La solución debe de utilizar Machine Learning y AI para detección de cambios de configuración sospechosos, permitiendo identificar patrones de ataques internos y externos antes de que causen impacto en la infraestructura.
PRODUCTIVIDAD	La solución debe de contar con optimización de recursos y rendimiento en estaciones de trabajo. • La solución debe de asegurar que no consuma recursos excesivos de memoria y procesador en los equipos de los usuarios, asegurando una ejecución optimizada incluso en estaciones con hardware limitado. • La solución debe de garantizar un uso eficiente de CPU y RAM mediante técnicas de Smart Scanning, asegurando que los procesos de escaneo y protección en tiempo real se ejecuten con baja prioridad en segundo plano para no afectar el desempeño del usuario. • La solución debe de ser compatible con entornos virtualizados y tecnología de Thin Clients, optimizando la ejecución en infraestructuras de VDI (Virtual Desktop Infrastructure). • La solución debe de contar con caché inteligente de archivos escaneados, evitando análisis redundantes y mejorando la velocidad del sistema. • La solución debe de optimizar el consumo de red, asegurando que las actualizaciones y parches se descarguen de manera distribuida (P2P) en redes locales para reducir el tráfico de Internet. • La solución debe de incluir capacidad de autoajuste de rendimiento, donde el sistema reduce el uso de recursos cuando detecta aplicaciones de alto consumo en ejecución (juegos, edición de video, herramientas CAD, etc.). • La solución debe de integrar una herramienta de mantenimiento automatizado, que incluya: • La solución debe de permitir desfragmentación del Registro de Windows, asegurando estabilidad y optimización del sistema operativo. • La solución debe de incluir desfragmentación del Disco Duro (HDD y SSD-aware optimization), evitando la fragmentación excesiva y mejorando los tiempos de acceso a datos. • La solución debe de contar con limpieza avanzada de Tracer Files (archivos temporales y residuos de software), evitando acumulaciones innecesarias en disco. • La solución debe de permitir escaneo y reparación de configuraciones dañadas del sistema operativo para garantizar su correcto funcionamiento. • La solución debe de incluir prevención de corrupción de archivos críticos del sistema mediante monitoreo proactivo y alertas anticipadas. • La solución debe de proporcionar optimización específica para unidades SSD, evitando operaciones de desfragmentación innecesarias que puedan acortar la vida útil del disco. • La solución debe de contar con modo de mantenimiento programado, asegurando que las tareas de optimización solo se ejecuten en horarios de baja actividad para no afectar la productividad del usuario. • La solución debe de incluir la capacidad de crear un disco de emergencia para desinfección avanzada de equipos con sistema operativo Microsoft Windows. • La solución debe de permitir que el disco de emergencia incluya: • La solución debe de contar con arranque en un entorno seguro basado en Linux o WinPE, permitiendo análisis forense sin que el sistema operativo infectado interfiera en la desinfección. • La solución debe de permitir escaneo y eliminación de malware, rootkits y bootkits antes de la carga del sistema operativo. • La solución debe de incluir herramientas de recuperación de archivos cifrados por ransomware, incluyendo descifrado y restauración desde copias de seguridad seguras. • La solución debe de contar con capacidad de restablecimiento de configuraciones críticas del sistema operativo en caso de corrupción. • La solución debe de ser compatible con UEFI y Secure Boot, permitiendo su uso en sistemas modernos sin necesidad de desactivar características de seguridad. • La solución debe de permitir gestión centralizada de actualizaciones de software, incluyendo: • La solución debe de administrar Microsoft Windows Updates (sin requerir WSUS), asegurando la aplicación de parches de seguridad críticos. • La solución debe de gestionar software de terceros como Adobe Reader, Flash, Java, Google Chrome, Mozilla Firefox, VLC, WinRAR, y otros software de productividad. • La solución debe de ser compatible con sistemas Linux y MacOS para mantener entornos multiplataforma actualizados. • La solución debe de contar con un mecanismo de escaneo proactivo de vulnerabilidades en software instalado, permitiendo: • La solución debe de detectar software desactualizado con parches de seguridad pendientes. • La solución debe de establecer priorización automática de actualizaciones críticas basadas en la severidad del CVE asociado.

	• La solución debe de generar reportes de conformidad de seguridad con información sobre aplicaciones vulnerables y recomendaciones de mitigación. • La solución debe de permitir parcheo incremental para minimizar el impacto en el rendimiento del sistema. • La solución debe de contar con rollback de parches en caso de fallas post-instalación, asegurando la estabilidad del sistema. • La solución debe de ofrecer control granular para definir qué estaciones reciben actualizaciones específicas según políticas corporativas. • La solución debe de contar con un sistema de actualización basado en IA, asegurando que los parches de seguridad se implementen de manera predictiva en función del riesgo y la criticidad. • La solución debe de incluir un mecanismo de autoaprendizaje (Machine Learning) que permite identificar qué estaciones requieren actualizaciones prioritarias en función de patrones de amenazas en la red. • La solución debe de permitir aplicar actualizaciones de seguridad incluso en equipos fuera de la red corporativa, permitiendo su sincronización mediante VPN, Cloud Proxy o servidores de distribución locales. • La solución debe de optimizar el uso de ancho de banda, permitiendo: • La solución debe de permitir actualizaciones distribuidas (P2P) en redes LAN. • La solución debe de programar parches en horarios fuera de producción. • La solución debe de aplicar compresión y optimización de descargas para minimizar el tráfico de red.
SOPORTE AL USUARIO	La solución debe de garantizar el cumplimiento de metas y especificaciones técnicas de la organización. • La solución debe de ser capaz de permitir al área de TI alcanzar las metas estratégicas de la empresa con exactitud, integridad y alineación con los estándares de ciberseguridad empresarial, asegurando: • La solución debe de cumplir con normativas internacionales de seguridad como ISO 27001, NIST 800-53, GDPR, PCI-DSS, HIPAA y otras regulaciones aplicables. • La solución debe de garantizar la integridad de la infraestructura TI, asegurando que todos los dispositivos y sistemas operen bajo políticas centralizadas de seguridad, minimizando riesgos de configuración errónea o incumplimiento de normativas internas. • La solución debe de proporcionar trazabilidad completa y auditoría de eventos de seguridad (SIEM & Log Management), generando registros detallados de todas las acciones realizadas en la infraestructura protegida. • La solución debe de permitir la gestión centralizada de la seguridad de endpoints, servidores, redes y aplicaciones, reduciendo la complejidad operativa y optimizando la administración del área de TI. • La solución debe de contar con un sistema de gestión y orquestación automatizada (Security Orchestration, Automation & Response - SOAR) que permita: • La solución debe de permitir la automatización de respuesta ante incidentes de seguridad, reduciendo el tiempo de reacción ante amenazas. • La solución debe de integrarse con herramientas de gestión de TI (ITSM) para reporte, seguimiento y resolución de incidentes. • La solución debe de implementar flujos de trabajo de seguridad basados en IA, garantizando cumplimiento de políticas sin intervención manual. • La solución debe de realizar análisis de comportamiento basado en Machine Learning para prevenir ataques internos o actividades sospechosas. • La solución debe de contar con capacidad de aplicar acciones correctivas automáticamente (aislamiento de dispositivos comprometidos, cierre de sesiones sospechosas, bloqueo de IPs maliciosas, etc.). • La solución debe de garantizar la precisión e integridad de los procesos de TI, asegurando: • La solución debe de proteger la configuración de sistemas críticos mediante control de cambios y validación criptográfica. • La solución debe de implementar políticas de Zero Trust Security, asegurando que ningún dispositivo o usuario acceda a recursos sin verificación previa. • La solución debe de validar la integridad del software y parches aplicados, evitando alteraciones no autorizadas. • La solución debe de supervisar y correlacionar eventos en tiempo real mediante integración con SIEM. • La solución debe de proporcionar control granular de accesos y auditoría con autenticación multifactor (MFA) y gestión de privilegios mínimos (PAM). • La solución debe de integrar capacidades de detección y respuesta ante amenazas con: • La solución debe de utilizar Threat Intelligence Feeds en tiempo real para prevenir ataques dirigidos y APTs (Advanced Persistent Threats). • La solución debe de realizar análisis heurístico y detección de amenazas emergentes basado en AI & Deep Learning.

	• La solución debe de monitorear el tráfico de red y proporcionar protección contra ataques basados en exploits y ransomware. • La solución debe de realizar escaneo de vulnerabilidades con integración a bases de datos CVE para priorización de parches de seguridad. • La solución debe de detectar intentos de evasión mediante técnicas de defensa avanzada contra malware polimórfico y ataques fileless. • La solución debe de facilitar la administración de la seguridad TI mediante: • La solución debe de generar reportes en tiempo real sobre el estado de la infraestructura, cumplimiento de políticas y métricas clave de ciberseguridad. • La solución debe de contar con capacidad de personalización y automatización de tareas administrativas para reducir la carga operativa del equipo de TI. • La solución debe de ser compatible con herramientas ITSM como ServiceNow, Jira, Remedy y otras plataformas de gestión de incidentes. • La solución debe de utilizar tecnologías de AI y Machine Learning para optimizar la identificación y remediación de problemas de seguridad. • La solución debe de garantizar interoperabilidad con soluciones de virtualización y entornos híbridos (VMware, Hyper-V, KVM, Docker, Kubernetes, etc.)

6. CONDICIONES DE CONTRATACIÓN

a. Modalidad de pago

El contrato se rige por la modalidad de A Suma Alzada y con Pago Único, de conformidad con el artículo 130 del reglamento.

b. Sistema de entrega

El contrato se rige por el sistema de entrega de Llave en mano de contratación, de conformidad con el artículo 129 del reglamento.

c. Plazo de entrega

Los bienes materia de la presente convocatoria se entregan en el plazo de diez (10) días calendarios, en concordancia con lo establecido en la estrategia de contratación.

d. Penalidades

Penalidad por mora:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

i. Recepción y Conformidad de la Prestación

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas. La recepción será otorgada por Unidad de Almacén Central y la conformidad será otorgada por la Oficina de Servicios Informáticos en el plazo máximo de siete (7), días computados desde el día siguiente de producida la recepción.

j. Solución de controversias contractuales:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje

Para el arbitraje el postor ganador de la buena pro selecciona a uno d ellos siguientes instituciones Arbitrales para administrar el Arbitraje.

Centro de Arbitraje y Conciliación del Colegio de Abogados de Lima.

Colegio de Ingenieros del Perú.

k. Gestión de Riesgos

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

Contratación de servicios: Al igual que en la compra de bienes, se podrían dar comportamientos irregulares como: (i) Favorecimiento indebido, (ii) Acceso a ventajas indebidas y (iii) Conflicto de intereses. (De corresponder el área usuaria, lo detallara en el numeral 4)

7. REQUISITOS DE CALIFICACION

A. CAPACIDAD LEGAL

Requisitos:

- Se requiere que la persona natural y/o jurídica este inscrita en el registro nacional de proveedores RNP en el rubro de bienes
- Contar con Registro Único de Contribuyente activo y habido
- Persona jurídica en el rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a paginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

Acreditación:

- RNP
- FICHA RUC

B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor deberá contar con la acreditación del fabricante, como partner y/o distribuidor autorizado de la solución de antivirus y antimalware corporativo propuesto, con lo cual garantizará las acciones necesarias ante algún incidente por infección por software malicioso ante el fabricante del producto ofertado.

Dicha condición deberá ser acreditado mediante carta y deberá ser presentada en la Propuesta Técnica, dirigida a la entidad convocante e indicando el número del proceso, en la cual indique que el proveedor es un distribuidor autorizado para su comercialización.

El postor debe acreditar un monto facturado acumulado equivalente a S/ 400,000.00 [Cuatrocientos mil con 00/100 soles], por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: ventas en adquisición de software antivirus y/o software de monitoreo y/o solución de antivirus y/o implementación de

plataformas de ciberseguridad en entornos hiperconvergentes con protección integral de endpoints y/o venta de licencias XDR y/o venta de licencias EDR, pueden incluir implementación y/o instalación y/o soporte y/o antimalware que incluye soporte para end point y/o soluciones de SSL-VPN.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (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, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o la cancelación del mismo con comprobante de pago , o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte primeras contrataciones indicadas en el Anexo Nº 11 referido a la Experiencia del Postor en la Especialidad.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los diez años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 14.

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad que le hubiesen transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo Nº 12 referido a la Experiencia del Postor en la Especialidad.

8. REQUISITOS DE CALIFICACION FACULTATIVOS

8.1. CAPACIDAD TÉCNICA Y PROFESIONAL

8.1.1. Experiencia del personal clave

Requisitos:

01 JEFE DE PROYECTO

- Profesional titulado en la carrera de ingeniería de sistemas, computación, estadística y/o informática y/o afines lo cual lo acreditara con copia del título profesional.
- Experiencia mínima de 3 años en la realización de este tipo de trabajo

01 ESPECILISTA

- Profesional titulado en la carrera de ingeniería de sistemas, computación, estadística y/o informática y/o afines lo cual lo acreditara con copia del título profesional.
- Experiencia mínima de 2 años en la realización de este tipo de trabajo

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.

Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

9. LUGAR DE ENTREGA:

- Almacén central de la Universidad Nacional José Faustino Sánchez Carrión.
- El proveedor deberá entregar los bienes con la guía de remisión correspondiente.

10. CONFORMIDAD

La conformidad estará a cargo del jefe de la Oficina de Servicios Informáticos. La conformidad deberá ser otorgada en un plazo no mayor de cinco (5) días hábiles.

11. RESPONSABILIDAD POR VICIOS OCULTOS

El PROVEEDOR será responsable por la calidad ofrecida y por los vicios ocultos por un plazo de uno (01 año) contado a partir de la conformidad otorgada por la Entidad.

12. RESOLUCIÓN DE CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

13. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación y/o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento.

JEFATURA

Ing. Oswaldo A. Romero Valladares
Jefe de la Oficina de Servicios Informáticos

FIRMA Y SELLO POSFIRMA

RESPONSABLE DEL ÁREA USUARIA

3.5 REQUISITOS DE CALIFICACIÓN

3.5.1. REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

A. CAPACIDAD LEGAL

Requisitos:

- Se requiere que la persona natural y/o jurídica este inscrita en el registro nacional de proveedores RNP en el rubro de bienes
- Contar con Registro Único de Contribuyente activo y habido
- Persona jurídica en el rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a páginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

Acreditación: Copia simple de:

- *RNP*
- *FICHA RUC*

Advertencia
En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.

B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor deberá contar con la acreditación del fabricante, como partner y/o distribuidor autorizado de la solución de antivirus y antimalware corporativo propuesto, con lo cual garantizará las acciones necesarias ante algún incidente por infección por software malicioso ante el fabricante del producto ofertado.
Dicha condición deberá ser acreditado mediante carta y deberá ser presentada en la Propuesta Técnica, dirigida a la entidad convocante e indicando el número del proceso, en la cual indique que el proveedor es un distribuidor autorizado para su comercialización.

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 400,000.00 (Cuatro cientos mil con 00/100 soles)**, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: ventas en adquisición de software antivirus y/o software de monitoreo y/o solución de antivirus y/o implementación de plataformas de ciberseguridad en entornos hiper convergentes con protección integral de endpoints y/o venta de licencias XDR y/o venta de licencias EDR, pueden incluir implementación y/o instalación y/o soporte y/o antimalware que incluye soporte para end point y/o soluciones de SSL-VPN.

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de (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, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o la

cancelación del mismo con comprobante de pago[6], o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[7], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte primeras contrataciones indicadas en el **Anexo Nº 11** referido a la Experiencia del Postor en la Especialidad.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los diez años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 14**.

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad que le hubiesen transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 12** referido a la Experiencia del Postor en la Especialidad.

Advertencia
En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto del contrato.

3.5.2. REQUISITOS DE CALIFICACIÓN FACULTATIVOS

C. CAPACIDAD TÉCNICA Y PROFESIONAL
C.1. Experiencia del personal clave

[6] El solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).
[7] Entendiéndose por estas a aquellos que no son entidades contratantes.

Requisitos:

01 JEFE DE PROYECTO

• Profesional titulado en la carrera de ingeniería de sistemas, computación, estadística y/o informática y/o afines lo cual lo acreditara con copia del título profesional.
• Experiencia mínima de 3 años en la realización de este tipo de trabajo

01 ESPECILISTA

• Profesional titulado en la carrera de ingeniería de sistemas, computación, estadística y/o informática y/o afines lo cual lo acreditara con copia del título profesional.
• Experiencia mínima de 2 años en la realización de este tipo de trabajo

Acreditación:
La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.

Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

ABSOLUCION DE CONSULTAS

PARTICIPANTE: SYMMETRY CORPORATION SOCIEDAD ANONIMA CERRADA

CONSULTA Nº 01:

Señores del comité, solicito se pueda aclarar con exactitud el plazo de entrega de los bienes mencionados.
Ya que se menciona un plazo de entrega de 5 días y 3 días para la instalación y puesta en funcionamiento. Por otro lado, en la página 34, numeral 6, literal C, en el plazo de entrega se menciona 10 días calendario.

Respuesta:

De acuerdo con el TDR, los plazos son los siguientes:

Plazo de entrega de los bienes

Numeral 6.c (Plazo de entrega): "Los bienes materia de la presente convocatoria se entregan en el plazo de diez (10) días calendarios, en concordancia con lo establecido en la estrategia de contratación."
Este plazo cubre la entrega física completa de las licencias y cualquier material asociado al antivirus en el Almacén Central de la Universidad.

Instalación y puesta en funcionamiento

La contratación se rige bajo modalidad 'llave en mano' (Numeral 6.b), lo que implica que tanto la entrega como la instalación y configuración final deben completarse dentro del mismo plazo global de 10 días calendario.
No existe un desdoble hay un error material de "3"dias para la instalación debe decir: "5 días para entrega" + "5 días para instalación": tales plazos están contemplados en el TDR.

Conclusión:
El único plazo vigente para la entrega e instalación completa "llave en mano" es de 10 días calendario contados desde la suscripción del contrato. Los supuestos plazos de 5 días y 5 días para instalación están definidos en el TDR Así mismo esta condición modifica el factor de evaluación plazo de entrega.

CONSULTA Nº 02:

Señores del comité, se solicita se pueda aclarar en cuanto a PUNTAJE/ METODOLOGÍA PARA SU ASIGNACIÓN, los 20 puntos en que aspecto se estarían brindando para PLAZO DE ENTREGA, no se menciona ello en el TDR.

Respuesta:

El factor de evaluación tiene como finalidad mejorar o superar el plazo de entrega, factor utilizado en cumplimiento de la Ley General de Contrataciones Ley Nº 32069

CONSULTA Nº 03:

Señores del comite, se solicita se pueda aclarar en cuanto a PUNTAJE/ METODOLOGÍA PARA SU ASIGNACIÓN, los 20 puntos en que aspecto se estarían brindando para CAPACITACIÓN AL PERSONAL DE LA ENTIDAD CONTRATANTE, no se menciona ello en el TDR.

Respuesta:

El factor de evaluación tiene como finalidad la de obtener la respectiva capacitación al personal de la oficina de servicios informáticos respecto a la funcionabilidad, alcances y las virtudes del antivirus, factor utilizado en cumplimiento de la Ley General de Contrataciones Ley Nº 32069

CONSULTA Nº 04:

Señores del comité, se solicita se pueda aclarar en cuanto a PUNTAJE/ METODOLOGÍA PARA SU ASIGNACIÓN, los 20 puntos en que aspecto se estarían brindando para MEJORAS A LAS ESPECIFICACIONES TÉCNICAS, no se menciona ello en el TDR.

Respuesta:

El factor de evaluación tiene como finalidad de mejorar y superar de ser el caso el plazo de la vigencia de los antivirus, factor utilizado en cumplimiento de la Ley General de Contrataciones Ley Nº 32069

CONSULTA Nº 05:

Señores del comité, se solicita se pueda aclarar en cuando al esquema del cuadro de las especificaciones técnicas cómo se distribuye para el antivirus de las computadoras y servidores, ya que lo colocan de manera unificada y general en el TDR.

Respuesta:

De acuerdo con los requisitos del TDR, el esquema de licenciamiento debe ofrecer flexibilidad total para proteger cualquier combinación de estaciones de trabajo y servidores, independientemente del sistema operativo (Windows, macOS o Linux). Para resolver la ambigüedad, se propone lo siguiente:

La solución debe implementar un pool único de licencias que permita asignar dinámicamente derechos de protección a servidores o estaciones de trabajo según se requiera, sin necesidad de comprar partidas separadas por sistema operativo o tipo de equipo.

Este modelo asegura portabilidad entre Windows, macOS y Linux, facilitando la reubicación de licencias en función de cambios en la infraestructura a futuro.
Desglose en el cuadro de Especificaciones Técnicas

Ítem	Plataforma	Cantidad de Licencias
Antivirus para servidores	Server	16
Antivirus para estaciones de trabajo		2088

Esta estructura deja claro cuántas licencias mínimas se reservan para servidores y para estaciones, a la vez que permite el reuso dinámico en cualquier plataforma.

PARTICIPANTE: ENTEL PERU S.A.

CONSULTA Nº 06:

En la base dice:
2.2.1.1. Documentos para la admisión de la oferta

Teniendo en cuenta lo dispuesto en la Resolución Directoral N.º 0015-2025-EF/54.01, que aprueba la Directiva N.º 0005-2025-EF/54.01,¿Directiva que establece las Bases estándar para los procedimientos de selección en el marco de la Ley N.º 32069, Ley General de Contrataciones Públicas¿, y considerando que el numeral 2.2.1.1 de dichas bases establece expresamente que ¿los evaluadores no pueden incorporar documentos adicionales a los establecidos en este acápite para la admisión de la oferta¿, solicitamos se sirvan confirmar que los únicos documentos exigibles para la admisión de la oferta son los expresamente señalados en el numeral 2.2.1.1.

Respuesta:

Se aclara que, en cumplimiento con la normativa vigente en contrataciones Ley Nº 32069 Ley General de Contrataciones Públicas, que los documentos exigibles para la ADMISION de la oferta están señalados en el numeral 2.2.1.1.

CONSULTA Nº 07:

En las bases dice:
FORMA DE PAGO

Agradeceremos se sirvan precisar la glosa que deberá consignarse en la FACTURA correspondiente a la contraprestación pactada, a fin de incluir la información correcta en el comprobante de pago a emitir

Respuesta:

Se aclara que el objeto de la contratación es: ADQUISICIÓN DE LICENCIAS SOFTWARE ANTIVIRUS PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LOS SERVIDORES DEL CENTRO DE DATOS PARA ASEGURAR LA CONTINUIDAD OPERATIVA DE LA UNIVERSIDAD, ASÍ COMO LA PROTECCIÓN DE TODAS LAS COMPUTADORAS DE LA UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN, es facultad y responsabilidad del Contratista para la contraprestación defina su glosa en la factura respectiva.

CONSULTA Nº 08:

En las bases dice:
FORMA DE PAGO

Solicitamos se sirvan confirmar si, en caso la Entidad no efectúe el pago de la contraprestación pactada dentro del plazo de tres (03) meses desde su exigibilidad, el contratista podría proceder con la suspensión temporal del acceso a las licencias contratadas, sin que ello conlleve la aplicación de penalidades ni afecte el porcentaje de cumplimiento del contrato, en caso corresponda.

Respuesta:

Se aclara que, el pago se realiza una vez otorgada la conformidad, el mismo que es en pago único, en virtud al artículo 67 de la Ley Nº 32069.

CONSULTA Nº 09:

En las bases dice:
FORMA DE PAGO

Agradeceremos confirmar y precisar que, para el pago de la contraprestación ejecutada, basta con que el contratista presente únicamente la FACTURA. Esto con el fin de tener claro este punto.

Respuesta:

Se aclara que, el pago se realiza una vez otorgada la conformidad, y lo tipificado en las bases numeral 2.4 del capítulo II DEL PROCEDIMIENTO DE SELECCIÓN, el mismo que es en pago único, en virtud al artículo 67 de la Ley Nº 32069.

CONSULTA Nº 10:

En las bases dice:
A. Capacidad Legal
Requisitos:
(¿)
Persona jurídica en el rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a páginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

En referencia del presente párrafo de requerimiento, agradeceremos confirmar que también se considerará válida la participación de personas jurídicas que desarrollan actividades económicas registradas como Actividades de telecomunicaciones inalámbricas y/o Actividades de

telecomunicaciones alámbricas y/o Venta al por menor de ordenadores, equipo periférico, programas de informática y equipos de telecomunicaciones en comercios especializados y/o dedicadas al rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a páginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

Respuesta:

Se aclara lo siguiente:
Actividades válidas
Solo se considerarán personas jurídicas cuya actividad económica principal esté comprendida en alguno de los rubros explícitos en el párrafo citado:
Tecnología de la información
Servicios informáticos
Venta de computadoras
Soluciones ligadas a páginas web
Licencias de software ofimática
Suministros informáticos
Consultoría de informática (o actividades similares al objeto)
Actividades no contempladas
Rechazamos expresamente incluir en la convocatoria a entidades cuya clasificación primaria sea:
Telecomunicaciones inalámbricas
Telecomunicaciones alámbricas
Venta al por menor de equipos de telecomunicaciones en comercios especializados
Estas actividades no se encuentran dentro del alcance definido en el primer párrafo de los TDR.
Aclaración sobre la solución propuesta
Asimismo, deseamos enfatizar que el objeto de esta contratación es una solución antimalware, la cual no guarda relación con servicios de telecomunicaciones ni venta de equipos de comunicación (segundo párrafo propuesto). Por tanto, cualquier postor deberá acreditar experiencia y capacidades específicas en soluciones antimalware y gestión de seguridad informática, conforme al objeto contractual.

CONSULTA Nº 11:

En las bases dice:
B. Experiencia del postor en la especialidad
Requisitos:
(¿)

Agradeceremos confirmar que como servicios similares también se aceptará la experiencia del postor en los siguientes servicios; ¿Licencia de Solución de Seguridad Antivirus¿ y/o "Servicio de Seguridad Gestionada" y/o "Servicio Integral de Telecomunicaciones" y/o "Servicio de Transmisión de Datos" y/o "Servicio de Acceso Dedicado a Internet y Enlace de Comunicación Punto a Punto" y/o "Servicio de Internet Dedicado y Enlace de Datos" y/o "Servicio de Conectividad a Internet mediante equipos modem" y/o ¿Servicio de Mensajería electrónica¿, esto con el fin de permitir una mayor concurrencia de postores y estar razonablemente justificada su admisión.

Respuesta:

Se aclara; con el objetivo de preservar la integridad y el enfoque técnico del procedimiento de selección, se aclara lo siguiente:
Servicios similares
Se considerará válida la participación de personas jurídicas que acrediten experiencia en alguno o varios de los siguientes ámbitos, siempre vinculados al objeto contractual de solución antimalware y gestión de seguridad de endpoints:
Venta y adquisición de software antivirus y/o software de monitoreo.
Suministro de soluciones de antivirus y/o plataformas de ciberseguridad en entornos hiperconvergentes con protección integral de endpoints.
Comercialización de licencias XDR y/o licencias EDR (incluida implementación, instalación y soporte).
Provisión de antimalware que contemple soporte para endpoint.
Implementación de soluciones SSL-VPN.

No califican como servicios similares:
No guardan relación directa con la protección antimalware ni la seguridad de endpoints. Desnaturalizan el objeto técnico de la contratación.
Pueden introducir criterios de evaluación ajenos al alcance de la licitación.
En consecuencia, no se admitirán como similares ni podrán subsanar requisitos de experiencia los siguientes:
"Servicio Integral de Telecomunicaciones"
"Servicio de Transmisión de Datos"
"Servicio de Acceso Dedicado a Internet y Enlace de Comunicación Punto a Punto"
"Servicio de Internet Dedicado y Enlace de Datos"
"Servicio de Conectividad a Internet mediante equipos módem"
"Servicio de Mensajería Electrónica"
Objeto del proceso
Recordamos que el presente procedimiento licitatorio tiene por objeto la contratación de una solución antimalware con gestión centralizada y protección de endpoints. Cualquier experiencia o servicio aportado debe estar estrictamente alineado con esta finalidad.

CONSULTA Nº 12:

En las bases dice:
Experiencia del personal clave.

Agradeceremos confirmar que independientemente de las denominaciones del (los) cargo(s) que ocupe o haya desempeñado el personal propuesto para el perfil del personal clave, se validará la experiencia del profesional conforme a sus funciones realizadas, en la medida que la constancia de trabajo señalará que el personal propuesto ha desarrollado las funciones o labores solicitadas independientemente de la denominación de los cargos fijados en las Bases

Respuesta:

En atención a su consulta, procedemos a aclarar lo siguiente:

Validación de experiencia y denominación de cargo
Conforme a lo establecido en las Bases, el personal propuesto deberá acreditar título profesional en las carreras indicadas y la experiencia mínima exigida para cada perfil:

Jefe de Proyecto: título profesional y ≥ 3 años de experiencia.
Especialista: título profesional y ≥ 2 años de experiencia.
Dicha acreditación comprende la revisión de la constancia de trabajo y del contenido de funciones desempeñadas.
Imposibilidad de flexibilidad en denominaciones
No es factible aceptar validaciones basadas únicamente en funciones descritas con denominaciones distintas a las previstas, dado que:
El cumplimiento de las labores específicas (gestión de proyectos antimalware y soporte especializado) exige conocimientos y competencias asociados a los perfiles titulados y certificados en las áreas señaladas.
En caso de un incidente de seguridad, resulta imperativo contar con profesionales cuya formación y experiencia coincidan de manera fehaciente con las funciones críticas definidas, garantizando una respuesta inmediata y efectiva.
Requisito de personal calificado
Por lo anterior, se mantiene la exigencia de que los cargos coincidan con los perfiles descritos en los TDR, sin posibilidad de sustitución o interpretación de títulos distintos, con el fin de salvaguardar la continuidad operativa y la integridad del servicio.

CONSULTA Nº 13:

En las bases dice:
Experiencia del personal clave.
(¿)

Experiencia mínima de 3 años en la realización de este tipo de trabajo.

Al respecto, con el fin de permitir una mayor concurrencia de postores con profesionales con experiencia en servicios similares al presente requerimiento, agradeceremos confirmar que será válido que el Jefe de Proyecto cuente con experiencia mínima de tres (03) años en ¿Gestión y supervisión de proyectos de implementación de servicios de transmisión de datos en general, banda ancha, internet y telecomunicaciones¿ y/o ¿Gestión y/o supervisión y/o coordinación de proyectos de telecomunicaciones tales como internet y/o internet dedicado¿.

Respuesta:

En atención a su consulta, procedemos a aclarar lo siguiente:
Validación de experiencia y denominación de cargo
Conforme a lo establecido en las Bases, el personal propuesto deberá acreditar título profesional en las carreras indicadas y la experiencia mínima exigida para cada perfil:
Jefe de Proyecto: título profesional y ≥ 3 años de experiencia.
Especialista: título profesional y ≥ 2 años de experiencia.
Dicha acreditación comprende la revisión de la constancia de trabajo y del contenido de funciones desempeñadas.
Imposibilidad de flexibilidad en denominaciones
No es factible aceptar validaciones basadas únicamente en funciones descritas con denominaciones distintas a las previstas, dado que:
El cumplimiento de las labores específicas (gestión de proyectos antimalware y soporte especializado) exige conocimientos y competencias asociados a los perfiles titulados y certificados en las áreas señaladas.

En caso de un incidente de seguridad, resulta imperativo contar con profesionales cuya formación y experiencia coincidan de manera fehaciente con las funciones críticas definidas, garantizando una respuesta inmediata y efectiva.
Requisito de personal calificado
Por lo anterior, se mantiene la exigencia de que los cargos coincidan con los perfiles descritos en los TDR, sin posibilidad de sustitución o interpretación de títulos distintos, con el fin de salvaguardar la continuidad operativa y la integridad del servicio.

CONSULTA Nº 14:

En las bases dice:
A. Capacidad Legal
Requisitos:
(¿)
Persona jurídica en el rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a páginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

En referencia del presente párrafo de requerimiento, agradeceremos confirmar que también se considerará válida la participación de personas jurídicas que desarrollan actividades económicas registradas como Actividades de telecomunicaciones inalámbricas y/o Actividades de telecomunicaciones alámbricas y/o Venta al por menor de ordenadores, equipo periférico, programas de informática y equipos de telecomunicaciones en comercios especializados y/o dedicadas al rubro de tecnología de la información y/o servicios informáticos y/o ventas de computadoras y/o soluciones ligadas a páginas web y/o licencias de software ofimática y/o suministros informáticos y/o consultoría de informática o similares al objeto de la contratación.

Respuesta:

Se aclara lo siguiente:
Actividades válidas
Solo se considerarán personas jurídicas cuya actividad económica principal esté comprendida en alguno de los rubros explícitos en el párrafo citado:

Tecnología de la información
Servicios informáticos
Venta de computadoras
Soluciones ligadas a páginas web
Licencias de software ofimática
Suministros informáticos
Consultoría de informática (o actividades similares al objeto)
Actividades no contempladas
Rechazamos expresamente incluir en la convocatoria a entidades cuya clasificación primaria sea:
Telecomunicaciones inalámbricas
Telecomunicaciones alámbricas
Venta al por menor de equipos de telecomunicaciones en comercios especializados
Estas actividades no se encuentran dentro del alcance definido en el primer párrafo de los TDR.
Aclaración sobre la solución propuesta
Asimismo, deseamos enfatizar que el objeto de esta contratación es una solución antimalware, la cual no guarda relación con servicios de telecomunicaciones ni venta de equipos de comunicación (segundo párrafo propuesto). Por tanto, cualquier postor deberá acreditar experiencia y capacidades específicas en soluciones antimalware y gestión de seguridad informática, conforme al objeto contractual.

CONSULTA Nº 15:

En las bases dice:
B. Experiencia del postor en la especialidad
Requisitos:
(¿)

Agradeceremos confirmar que como servicios similares también se aceptará la experiencia del postor en los siguientes servicios; ¿Licencia de Solución de Seguridad Antivirus¿ y/o "Servicio de Seguridad Gestionada" y/o "Servicio Integral de Telecomunicaciones" y/o "Servicio de Transmisión de Datos" y/o "Servicio de Acceso Dedicado a Internet y Enlace de Comunicación Punto a Punto" y/o "Servicio de Internet Dedicado y Enlace de Datos" y/o "Servicio de Conectividad a Internet mediante equipos modem" y/o ¿Servicio de Mensajería electrónica¿, esto con el fin de permitir una mayor concurrencia de postores y estar razonablemente justificada su admisión.

Respuesta:

En atención a su consulta, y con el objetivo de preservar la integridad y el enfoque técnico del proceso de selección, procedemos a aclarar lo siguiente:
Servicios similares aceptables
Se considerará válida la participación de personas jurídicas que acrediten experiencia en alguno o varios de los siguientes ámbitos, siempre vinculados al objeto contractual de solución antimalware y gestión de seguridad de endpoints:
Venta y adquisición de software antivirus y/o software de monitoreo.
Suministro de soluciones de antivirus y/o plataformas de ciberseguridad en entornos hiperconvergentes con protección integral de endpoints.
Comercialización de licencias XDR y/o licencias EDR (incluida implementación, instalación y soporte).
Provisión de antimalware que contemple soporte para endpoint.
Implementación de soluciones SSL-VPN.
Actividades excluidas
Se rechaza expresamente la consideración de los siguientes servicios, dado que:
No guardan relación directa con la protección antimalware ni la seguridad de endpoints.
Desnaturalizan el objeto técnico de la contratación.
Pueden introducir criterios de evaluación ajenos al alcance de la licitación.
En consecuencia, no se admitirán como similares ni podrán subsanar requisitos de experiencia los siguientes:
“Servicio Integral de Telecomunicaciones”
“Servicio de Transmisión de Datos”
“Servicio de Acceso Dedicado a Internet y Enlace de Comunicación Punto a Punto”
“Servicio de Internet Dedicado y Enlace de Datos”

"Servicio de Conectividad a Internet mediante equipos módem"
"Servicio de Mensajería Electrónica"
Objeto del proceso
Recordamos que el presente procedimiento licitatorio tiene por objeto la contratación de una solución antimalware con gestión centralizada y protección de endpoints. Cualquier experiencia o servicio aportado debe estar estrictamente alineado con esta finalidad.

CONSULTA Nº 16:

En las bases dice:
C.1. Experiencia del personal clave.

Agradeceremos confirmar que independientemente de las denominaciones del (los) cargo(s) que ocupe o haya desempeñado el personal propuesto para el perfil del personal clave, se validará la experiencia del profesional conforme a sus funciones realizadas, en la medida que la constancia de trabajo señalará que el personal propuesto ha desarrollado las funciones o labores solicitadas independientemente de la denominación de los cargos fijados en las Bases

Respuesta:

En atención a su consulta, procedemos a aclarar lo siguiente:

Validación de experiencia y denominación de cargo
Conforme a lo establecido en las Bases, el personal propuesto deberá acreditar título profesional en las carreras indicadas y la experiencia mínima exigida para cada perfil:

Jefe de Proyecto: título profesional y ≥ 3 años de experiencia.
Especialista: título profesional y ≥ 2 años de experiencia.
Dicha acreditación comprende la revisión de la constancia de trabajo y del contenido de funciones desempeñadas.
Imposibilidad de flexibilidad en denominaciones
No es factible aceptar validaciones basadas únicamente en funciones descritas con denominaciones distintas a las previstas, dado que:
El cumplimiento de las labores específicas (gestión de proyectos antimalware y soporte especializado) exige conocimientos y competencias asociados a los perfiles titulados y certificados en las áreas señaladas.
En caso de un incidente de seguridad, resulta imperativo contar con profesionales cuya formación y experiencia coincidan de manera fehaciente con las funciones críticas definidas, garantizando una respuesta inmediata y efectiva.

CONSULTA Nº 17:

En las bases dice:
C.1. Experiencia del personal clave.

(¿)
Experiencia mínima de 3 años en la realización de este tipo de trabajo.

Al respecto, con el fin de permitir una mayor concurrencia de postores con profesionales con experiencia en servicios similares al presente requerimiento, agradeceremos confirmar que será válido que el Jefe de Proyecto cuente con experiencia mínima de tres (03) años en ¿Gestión y supervisión de proyectos de implementación de servicios de transmisión de datos en general, banda ancha, internet y telecomunicaciones¿ y/o ¿Gestión y/o supervisión y/o coordinación de proyectos de telecomunicaciones tales como internet y/o internet dedicado¿.

Respuesta:

En atención a su consulta, procedemos a aclarar lo siguiente:

Validación de experiencia y denominación de cargo
Conforme a lo establecido en las Bases, el personal propuesto deberá acreditar título profesional en las carreras indicadas y la experiencia mínima exigida para cada perfil:
Jefe de Proyecto: título profesional y ≥ 3 años de experiencia.
Especialista: título profesional y ≥ 2 años de experiencia.
Dicha acreditación comprende la revisión de la constancia de trabajo y del contenido de funciones desempeñadas.
Imposibilidad de flexibilidad en denominaciones
No es factible aceptar validaciones basadas únicamente en funciones descritas con denominaciones distintas a las previstas, dado que:
El cumplimiento de las labores específicas (gestión de proyectos antimalware y soporte especializado) exige conocimientos y competencias asociados a los perfiles titulados y certificados en las áreas señaladas.
En caso de un incidente de seguridad, resulta imperativo contar con profesionales cuya formación y experiencia coincidan de manera fehaciente con las funciones críticas definidas, garantizando una respuesta inmediata y efectiva.

CONSULTA Nº 18:

En la base dice:
B. PLAZO DE ENTREGA

Evaluación:
(¿.)

Acreditación:
Se acreditará mediante la presentación de declaración jurada de plazo de prestación del servicio. (Anexo Nº 12)

Con el propósito de asegurar la correcta presentación de los Anexos que forman parte de la oferta, agradeceremos confirmar que el Anexo N.º 12 debe ser completado conforme a los plazos indicados en el literal C. Plazo de Entrega del numeral 3.3 CONDICIONES DE CONTRATACIÓN de las bases, consignando además el plazo de entrega ofertado por el postor para la entrega los bienes, a fin de que dicho plazo pueda ser considerado en la evaluación y asignación de puntaje correspondiente.

Respuesta:

SE ACLARA QUE EL PLAZO DE ENTREGA ES ACREDITADO EN EL ANEXO Nº 12 DENOMINADO DECLARACION JURADA DE PLAZO DE ENTREGA, COMO FACTOR DE EVALUACION DISTINTO A LO TIPIFICADO EN EL REQUERIMIENTO.

CONSULTA Nº 19:

En la base dice:
ANEXO N.º 6.
PRECIO DE LA OFERTA
(¿)
Concepto

Agradeceremos confirmar y precisar que el objeto de la convocatoria que debe consignarse en el detalle del concepto requerido en el Anexo N.º 6.corresponde al señalado en el numeral 1.3 Objeto de la convocatoria: ¿La contratación para la adquisición de licencias de software antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos, para Asegurar la Continuidad Operativa de la Universidad, Así como la Protección de todas las Computadoras de la

Universidad Nacional José Faustino Sánchez Carrión.¿ Ello, con el fin de completar de manera adecuada el Anexo N.º 6.

Respuesta:

Se aclara que, el llenado del anexo Nº 6 PRECIO DE LA OFERTA, es competencia y responsabilidad del postor.

CONSULTA Nº 20:

En los terminos de referencia se indica:
- SISTEMAS OPERATIVOS:
Windows Server 2012 (Standard / Essentials / Foundation / Storage Server / Datacenter) (64 bits) Windows Server 2008 R2 (Web/ Estándar/Empresa / Datacenter) (64 bits) Windows Server 2008 (Web/Estándar / Empresarial) (32 bits/ 64 bits) / Datacenter (64 bits)

Consulta: Se solicita a la entidad que las versiones de Windows Server 2008 y 2012 sean descartadas por temas de seguridad. Asimismo se solicita a la entidad indicar que sistemas operativos manejan en la actualidad.

Respuesta:

Imposibilidad de descartar Windows Server 2008 y 2012

Según el numeral 5 (Especificaciones Técnicas > Sistemas Operativos) del TDR, la solución debe ofrecer compatibilidad con Windows Server 2008 (Web/Estándar/Empresarial/Datacenter) y Windows Server 2012 (Standard/Essentials/Foundation/Storage Server/Datacenter) en sus distintas ediciones y arquitecturas.

Eliminar dichas versiones implicaría dejar fuera de cobertura parte de la plataforma actual de servidores del Centro de Datos, generando un riesgo operativo inaceptable que contraviene el Objetivo de la Adquisición (punto 3) de “asegurar la continuidad operativa de la universidad”.

Por tanto, esta propuesta se rechaza: mantener ambas versiones es indispensable para garantizar la protección integral de todos los servidores existentes y cumplir la finalidad pública de “garantizar la seguridad cibernética y la integridad de los sistemas de información” (punto 4).

Inventario de sistemas operativos en uso
Para respaldar el alcance definido en el TDR, la Oficina de Servicios Informáticos certifica que la infraestructura de servidores del Centro de Datos incluye actualmente:

Windows Server 2012 R2 (Estándar y Datacenter)

Windows Server 2016 (Estándar y Datacenter)

Windows Server 2019 (Estándar)

Estas versiones, junto con Windows Server 2008 y 2012, forman parte del parque existente y, por tanto, deben mantenerse en el TDR para asegurar que la solución antivirus cubra al 100 % los sistemas críticos de la Universidad.

CONSULTA Nº 21:

En los terminos de referencia se indica:
- SISTEMAS OPERATIVOS:
Ubuntu 16.04, 18.04, 20.04, 22.04, 23.10 Debian 9, 10, 11, 12
CentOS 7.8, 8.2, Stream 8, Stream 9
RHEL 7.5, 7.8, 8.2, 8.6, 9.0, 9.2 Enterprise

Consulta: Se solicita a la entidad que la posibilidad de instalacion sobre versiones antiguas o descontinuadas como son RedHat Enterprise Linux (RHEL) 7, CentOS 7, Ubuntu Server 18.04 y Debian10 sean opcionales.

Respuesta:

Obligatoriedad según TDR
El numeral 5 (Especificaciones Técnicas – Sistemas Operativos) del TDR incluye de manera expresa y obligatoria las versiones:

RHEL 7.5/7.8

CentOS 7.8

Ubuntu 18.04

Debian 10
Estas ediciones están listadas de forma no facultativa, por lo que deben cubrirse integralmente.

Continuidad operativa y cobertura total
El Objetivo de la Adquisición (punto 3) y la Finalidad Pública (punto 4) exigen proteger la totalidad de los sistemas en producción. Marcar dichas versiones como "opcionales" dejaría fuera de amparo entornos que aún forman parte del parque instalado, generando un riesgo operativo inaceptable.

Riesgo de incompatibilidad futura
Permitir soluciones que omitan estos sistemas comprometería la integridad y disponibilidad de servidores legados, contrariando el principio de "continuidad operativa" y la directiva de "protección integral de todos los sistemas y computadoras" especificada en el TDR.

Conclusión:
La solicitud de hacer opcional la compatibilidad con RHEL 7, CentOS 7, Ubuntu 18.04 y Debian 10 se rechaza, dado que dichas versiones están definidas como requisitos técnicos obligatorios en el TDR para garantizar la cobertura completa y continuidad operativa de la Universidad.

CONSULTA Nº 22:

En los terminos de referencia se indica:
-La solución debe de permitir instalación remota, gestión centralizada y descubrimiento automático de equipos.
¿ La solución debe de permitir instalación remota desde una herramienta del propio fabricante, asegurando un despliegue automatizado, seguro y escalable en todos los equipos dentro de la infraestructura de TI.

Consulta: Se solicita a la entidad confirmar si la instalación del agente de seguridad puede realizarse mediante métodos automatizados como GPO, SCCM o mediante consola web del fabricante, considerando entornos híbridos (on-premise y nube).

Respuesta:

Conforme al numeral 5 (Especificaciones Técnicas) – INSTALACIÓN del TDR:

Instalación remota desde herramienta del fabricante

La solución debe "permitir instalación remota desde una herramienta del propio fabricante, asegurando un despliegue automatizado, seguro y escalable en todos los equipos…"

Compatibilidad con métodos automatizados

Se establece expresamente que la solución debe ser “compatible con herramientas de gestión de despliegue como SCCM, Ansible, Puppet, Chef y Microsoft Intune”.

Además, debe “sincronizarse con Active Directory para despliegue automatizado en entornos Windows y Azure AD”, lo cual habilita el uso de GPO y otros mecanismos basados en políticas de dominio.

Entornos híbridos on-premise y nube

El TDR incluye soporte de “Microsoft Hyper-V (incluyendo entornos en Azure)” y “gestión centralizada de equipos remotos (clientes roaming) sin exponer la consola en DMZ”, garantizando cobertura tanto local como en la nube.

Conclusión:
La instalación del agente sí puede realizarse mediante GPO, SCCM o consola web del fabricante, y dichos métodos están plenamente amparados dentro del esquema de instalación remota y gestión centralizada exigido por el TDR para entornos on-premise y cloud.

CONSULTA Nº 23:

En los terminos de referencia se indica:
- La solución debe de ser compatible con UEFI y Secure Boot, permitiendo su uso en sistemas modernos sin necesidad de desactivar caracteristicas de seguridad.

Consulta: Sírvase la entidad a confirmar si se acepta que la compatibilidad con UEFI y Secure Boot esté sujeta a las políticas de arranque seguro del sistema operativo y hardware utilizado.

Respuesta:

Sujeción a políticas de arranque seguro
Efectivamente, la compatibilidad con UEFI y Secure Boot debe respetar las políticas nativas de firmware y sistema operativo de cada plataforma. La solución antivirus no podrá exigir la desactivación de Secure Boot ni la instalación de componentes no firmados: debe ajustarse al modelo de confianza que imponga el hardware y el S.O.
Requisito de firma y validación
El proveedor debe suministrar todos los binarios y controladores firmados con certificados válidos para UEFI Secure Boot, de modo que el agente se cargue automáticamente en entornos con arranque seguro habilitado, sin intervenciones manuales ni modificaciones de políticas.
Demostración de cumplimiento
Para garantizar el cumplimiento, se exige al postor:
Informe técnico que detalle el esquema de firma UEFI y la cadena de confianza empleada.
Pruebas de laboratorio en al menos tres modelos de hardware (por ejemplo, servidores HP, Dell y Lenovo) con Secure Boot activado, mostrando arranques exitosos del agente antivirus.
Con lo anterior, se confirma que la solución opera bajo las restricciones de Secure Boot de cada plataforma, sin requerir su desactivación, tal como exige el TDR.

CONSULTA Nº 24:

En los terminos de referencia se indica:
- La solución debe de incluir herramientas de recuperación de archivos cifrados por ransomware, incluyendo descifrado y restauración desde copias de seguridad seguras.
¿ La solución debe de contar con capacidad de restablecimiento de configuraciones críticas de! sistema operativo en caso de corrupción.

Consulta: Sírvase la entidad a confirmar si la funcionalidad de escaneo y remediación en entorno seguro puede realizarse mediante herramientas del fabricante que no requieren ejecución directa en el sistema comprometido (modo rescate)

Respuesta:

"Se propone denegar la obligación de incluir una herramienta de recuperación de archivos cifrados por ransomware."

No procede. El TDR estipula de manera explícita la incorporación de "herramientas de recuperación de archivos cifrados por ransomware, incluyendo descifrado y restauración desde copias de seguridad seguras" y "capacidad de restablecimiento de configuraciones críticas del sistema operativo en caso de corrupción".

Alcance mínimo obligatorio

La finalidad pública señalada en el numeral 3 ("asegurar la continuidad operativa de la universidad") impone disponer de mecanismos de recuperación íntegros tras un incidente de ransomware.

Omitir dicha herramienta contraviene el objetivo de "proteger la información crítica" y la "continuidad de las operaciones" descritos en los numerales 3 y 4 del TDR.

Riesgo operativo inaceptable

Sin un módulo de recuperación dedicado, no es posible garantizar tiempos de respuesta adecuados ni restauración confiable de datos cifrados.

La ausencia de esta funcionalidad incrementa exponencialmente el riesgo de pérdida de información académica y administrativa, contraponiéndose a los principios de integridad y resiliencia corporativa exigidos.

En consecuencia, se rechaza la propuesta de denegar esta obligación. La solución debe incluir de forma obligatoria la herramienta de recuperación contra ransomware tal como se especifica en el TDR.

CONSULTA Nº 25:

En los terminos de referencia se indica:
- ¿ La solución debe de cumplir con normativas internacionales de seguridad como ISO 27001,NIST 800-53, GDPR, PCI-DSS, HIPAA y otras regulaciones aplicables.

Consulta:Sírvase la entidad a confirmar si

Respuesta:

Se acoge a la consulta el cumplimiento con normas ISO 27001, NIST 800-53 y GDPR puede acreditarse mediante certificaciones del fabricante y no exclusivamente del postor.

CONSULTA Nº 26:

En los terminos de referencia se indica:
- La solución debe de ser compatible con herramientas ITSM como ServiceNow, Jira, Remedy y otras plataformas de gestión de incidentes.

Consulta:Sírvase la entidad a confirmar si se acepta como válida la integración con herramientas ITSM como ServiceNow, Jira o Remedy a través de API públicas o conectores certificados por el fabricante.

Respuesta:

Se aclara que; Instalación remota desde herramienta del fabricante

PARTICIPANTE: CORPORACION DIGI ARCH PERU SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA

CONSULTA Nº 27:

Confirmar cual es la version actual de la solucion antivirus con la que cuenta la entidad

Respuesta:

"Confirmar cuál es la versión actual de la solución antivirus con la que cuenta la entidad."

Por razones de seguridad de la información y preservación de la confidencialidad del entorno de la Universidad, no se publicará la versión exacta de la solución antivirus en los términos de referencia.

La información detallada sobre la versión vigente y los parámetros de configuración se proporcionará únicamente al adjudicatario del proceso, en el marco de la firma del contrato y con las garantías de acceso seguro establecidas en las políticas institucionales.

De esta manera, se asegura que únicamente personal debidamente acreditado y el proveedor ganador tengan visibilidad de esos datos críticos, mitigando riesgos operativos y de ciberseguridad.

CONSULTA Nº 28:

Confirmar para acreditar el cumplimiento de las especificaciones tecnicas se aceptara carta del fabricante donde se confirme el cumplimiento de los requerimientos tecnicos solicitados en las bases del procedimiento

Respuesta:

Se aclara que para el cumplimiento de las especificaciones técnicas la carta del fabricante es opcional

CAPÍTULO IV
FACTORES DE EVALUACIÓN

Los factores de evaluación son determinados por los evaluadores. La evaluación se realiza sobre la base de cien puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:

2.1. FACTOR DE EVALUACIÓN OBLIGATORIO

A. OFERTA ECONÓMICA

FACTOR DE EVALUACIÓN ECONÓMICO	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6).**	La evaluación consistirá en otorgar el mayor puntaje a la oferta del menor monto y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos montos ofertados, según la siguiente fórmula: $Po = \frac{Mb \times Pmax}{Mo}$ **Po** = Puntaje de la oferta económica a evaluar **Mo** = Monto de la oferta económica **Mb** = Monto de la oferta económica más baja **Pmax** = **40 puntos** **Puntaje máximo**

2.2. FACTORES DE EVALUACIÓN FACULTATIVOS

B. PLAZO DE ENTREGA	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
Evaluación: Se evaluará en función al plazo de entrega ofertado, el cual debe mejorar el plazo de entrega establecido en el requerimiento. Acreditación: Se acreditará mediante la presentación de declaración jurada de plazo de entrega. **(Anexo Nº 12)** **Advertencia** *En el caso del sistema de entrega llave en mano o llave en mano con mantenimiento, el plazo de entrega incluye además la instalación y puesta en funcionamiento, pero se evalúa el plazo correspondiente a la entrega del bien.*	**20 puntos** De **7** hasta **9** días calendario: **15 puntos** De **4** hasta **6** días calendario: **20 puntos**

I. CAPACITACIÓN AL PERSONAL DE LA ENTIDAD CONTRATANTE	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
Evaluación: Se evaluará en función a la oferta de capacitación a cuatro personas (OSI), en la sala de reuniones de la Oficina de Servicios informáticos de la Universidad, materia objeto del	**20 puntos** Más de 1 hora académica: **10 puntos** Más de 2 horas académica: **15 puntos**

requerimiento (Antivirus), la capacitación será de manera presencial por personal idóneo y con conocimiento acreditado para la capacitación. El postor que oferte esta capacitación se obliga a entregar los certificados o constancias del personal capacitado a la entidad contratante. **Advertencia** *Las calificaciones del capacitador que se pueden requerir son el grado académico de bachiller o título profesional, así como, de ser el caso, experiencia no mayor de dos años, vinculada a la materia de la capacitación relacionada con la operatividad de los bienes a ser contratados.* Acreditación: Se acreditará únicamente mediante la presentación de una declaración jurada.	Más de 3 horas académicas: **20 puntos**

J. MEJORAS A LAS ESPECIFICACIONES TÉCNICAS	**PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN**
Evaluación: 1.- Al postor que oferte 15 días más de vigencia del antivirus una vez culminado el contrato 2.- Al postor que oferte 30 días más de vigencia del antivirus una vez culminado el contrato **Acreditación:** Se acreditará únicamente mediante la presentación de una declaración jurada dirigida al oficial de compra **Advertencia** *Constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en el requerimiento, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la entidad contratante.*	**20 puntos** Mejora 1: **10 puntos** Mejora 2: **20 puntos**

CUADRO RESUMEN FACTORES DE EVALUACIÓN

FACTORES DE EVALUACIÓN OBLIGATORIOS	**PUNTAJE**
A. OFERTA ECONÓMICA	[Máximo 40] puntos
FACTORES DE EVALUACIÓN FACULTATIVOS	**PUNTAJE**
B. PLAZO DE ENTREGA	**[mínimo 15] puntos / NO CORRESPONDE**
C. SOSTENIBILIDAD ECONÓMICA	**[máximo 5] puntos / NO CORRESPONDE**
D. SOSTENIBILIDAD SOCIAL	**[máximo 5] puntos / NO CORRESPONDE**
E. SOSTENIBILIDAD AMBIENTAL	**[máximo 5] puntos / NO CORRESPONDE**
F. INTEGRIDAD EN LA CONTRATACIÓN PÚBLICA	**[máximo 5] puntos / NO CORRESPONDE**
G. GARANTÍA COMERCIAL DEL POSTOR	**[mínimo 15] puntos / NO CORRESPONDE**
H. DISPONIBILIDAD DE SERVICIOS Y RESPUESTOS	**[mínimo 15] puntos / NO CORRESPONDE**
I. CAPACITACIÓN AL PERSONAL DE LA ENTIDAD CONTRATANTE	**[mínimo 15] puntos / NO CORRESPONDE**
J. MEJORAS A LAS ESPECIFICACIONES TÉCNICAS	**[mínimo 15] puntos / NO CORRESPONDE**
K. VIDA ÚTIL DEL BIEN	**[mínimo 15] puntos / NO CORRESPONDE**
PUNTAJE TOTAL	**100 puntos**[8]

[8] Es la suma de los puntajes de todos los factores de evaluación.

CAPÍTULO V
PROFORMA DEL CONTRATO

Advertencia
Dependiendo del objeto de la contratación, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.

Conste por el presente documento, la contratación para la **Adquisición de Licencias Software Antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos para Asegurar la Continuidad Operativa de la Universidad, así como la Protección de todas las Computadoras de la Universidad Nacional José Faustino Sánchez Carrión,** que celebra de una parte la **Universidad Nacional José Faustino Sánchez Carrión,** en adelante LA ENTIDAD CONTRATANTE, con **RUC Nº 20172299742**, con domicilio legal en **Av. Mercedes Indacochea N° 600 Huacho**, representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° […….....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el oficial de compras adjudico la buena pro de la **LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC,** para la contratación **de Licencias Software Antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos para Asegurar la Continuidad Operativa de la Universidad, así como la Protección de todas las Computadoras de la Universidad Nacional José Faustino Sánchez Carrión** a [**INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO**], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por finalidad la **Adquisición de Licencias Software Antivirus para la Protección de los Sistemas de Información de los Servidores del Centro de Datos para Asegurar la Continuidad Operativa de la Universidad, así como la Protección de todas las Computadoras de la Universidad Nacional José Faustino Sánchez Carrión.**

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [**CONSIGNAR MONEDA Y MONTO**], que incluye todos los impuestos de Ley.

Este monto comprende el costo del bien, todos los tributos, seguros, transporte, 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 la ejecución de la prestación materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO[9]

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, en **PAGO ÚNICO,** luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[9] En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días del día siguiente de recibido el bien, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

LA ENTIDAD CONTRATANTE debe efectuar el pago dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

En caso de retraso en el pago por parte de LA ENTIDAD CONTRATANTE, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la N°32069, Ley General de Contrataciones Pública.

Importante para la entidad contratante

- *En caso de que la ENTIDAD CONTRATANTE verifique en la Pladicop que el CONTRATISTA tiene multas impagas que no se encuentren en procedimiento coactivo, se debe incluir la siguiente cláusula:*

CLÁUSULA QUINTA: COMPROMISO DE PAGO DE MULTA
Durante la ejecución del contrato la ENTIDAD CONTRATANTE retiene al CONTRATISTA de forma prorrateada hasta el 10% del monto del contrato, para el pago o amortización de multas impagas impuestas de en el marco de lo previsto en el artículo 89 de la Ley N° 32069, que no se encuentran en procedimiento coactivo.

- *En el caso que, adicionalmente, el proveedor presente la DECLARACIÓN JURADA SOBRE INAPLICACIÓN DEL IMPEDIMENTO TIPO 4.D DEL INCISO 4 DEL NUMERAL 30.1 DEL ARTÍCULO 30 DE LA LEY N° 32069 REFERIDO A LA INSCRIPCIÓN EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS – REDAM que autoriza descuento para el pago de deuda alimentaria, se debe indicar la siguiente cláusula:*

CLÁUSULA []: AUTORIZACIÓN DE DESCUENTO DE PENSIÓN ALIMENTARIA

*EL CONTRATISTA autoriza que se le descuente del pago de su contraprestación el monto de la pensión mensual fijada en el proceso de alimentos ascendiente a **[CONSIGNAR MONTO]**seguido por **[CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS]** ante el [**CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO CORRESPONDIENTE]** en el trámite del expediente **[CONSIGNAR EL NÚMERO DE EXPEDIENTE JUDICIAL].***

.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN
El plazo de ejecución del presente contrato es de [……..], el mismo que se computa desde EL **DÍA SIGUIENTE LA NOTIFICACIÓN DE LA ORDEN DE COMPRA. SISTEMA DE ENTREGA DE LLAVE EN MANO EL PLAZO DE ENTREGA (5 DIAS) Y LA INSTALACION (3 DIAS), SU INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y MANTENIMIENTO,**

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO
El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes, incluyendo las modificaciones contractuales y adendas aprobadas por la entidad contratante, de ser el caso.

CLÁUSULA SÉTIMA: GARANTÍAS
EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD CONTRATANTE, por los conceptos, montos y vigencias siguientes:

Garantía de fiel cumplimiento del contrato: Por la suma de [**CONSIGNAR EL MONTO**], a

través de la **[INDICAR EL MECANISMO DE GARANTÍA PRESENTADA: CONTRATO DE SEGURO/CARTA FIANZA FINANCIERA/RETENCIÓN DE PAGO/DECLARACIÓN JURADA DE CONSTITUCIÓN DE FIDEICOMISO]** N° [**INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE**], la misma que debe mantenerse vigente hasta la conformidad de la conformidad de la prestación. El monto señalado es equivalente al diez por ciento (10%) del monto del contrato original.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD CONTRATANTE puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el artículo 118 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas. La recepción será otorgada por la Unidad de Almacén Central y la conformidad será otorgada por la Oficina de Servicio Informáticos en el plazo máximo de **SIETE (7) DÍAS O DE VEINTE (20) DÍAS, ESTO ÚLTIMO EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN**] días computados desde el día siguiente de producida la recepción.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar el cual no debe ser mayor al 30% del plazo del entregable [10] correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD CONTRATANTE no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA UNDÉCIMA: GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de UN AÑO contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD CONTRATANTE le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula:

[10] En caso de que el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad contratante efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto.

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde:

F = 0.40

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD CONTRATANTE puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso

de contratación[11] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[12]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[13]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[14].

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

El marco legal comprende la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado por Decreto Supremo N° 009-2025-EF, las directivas que emita la Dirección General de Abastecimiento del Ministerio de Economía y Finanzas, así como el OECE y demás normativa especial que resulte aplicable.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS[15]

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante CONCILIACION Y/O ARBITRAJE, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas.

CLÁUSULA DÉCIMA NOVENA: CONVENIO ARBITRAL

Las partes acuerdan que todo litigio y controversia resultante de este contrato o relativo a éste, se resolverá mediante arbitraje de acuerdo con los artículos 332 y 333 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. El arbitraje es organizado y administrado por [**CONSIGNAR LA INSTITUCIÓN ARBITRAL, CORTE ARBITRAL CONSTITUÍDA EN OTRO PAÍS O UN FORO DE REPUTACIÓN RECONOCIDA INTERNACIONALMENTE, SEGÚN CORRESPONDA**] de conformidad con sus reglamentos y estatutos vigentes, a los cuales las partes se someten libremente y considerando [**INDICAR LAS**

[11] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

[12] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[13] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas
[14] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.
[15] De acuerdo con el numeral 84.1 del artículo 84 de la Ley General de Contrataciones Públicas, las partes pueden recurrir al arbitraje ad hoc solo cuando el monto de la controversia no supere las diez UIT.

ESTIPULACIONES ADICIONALES QUE LAS PARTES HAYAN ACORDADO SEGÚN EL NUMERAL 332.3 DEL ARTÍCULO 332 DEL REGLAMENTO DE LA LEY N° 32069, LEY GENERAL DE CONTRATACIONES PÚBLICAS, APROBADO POR DECRETO SUPREMO N° 009-2025-EF].

Advertencia

La Institución Arbitral es elegida por el postor ganador de la buena pro de la lista de instituciones arbitrales que haya propuesto la entidad contratante en las bases del procedimiento de selección. Para dicho efecto, al remitir los documentos para la suscripción del contrato, el postor ganador de la buena pro comunica la Institución Arbitral elegida de la referida lista, caso contrario, acuerda con la entidad contratante una Institución Arbitral distinta. En caso de falta de acuerdo, la Institución Arbitral es elegida de la mencionada lista por la entidad contratante de manera definitiva.

Las partes pueden establecer estipulaciones adicionales o modificatorias del convenio arbitral, en la medida que no contravengan las disposiciones de la normativa de contrataciones públicas y/o las disposiciones especiales contenidas en la normativa general de arbitraje.

El arbitraje es resuelto por árbitro único o por un tribunal arbitral conformado por tres árbitros, según el acuerdo de las partes, conforme a lo dispuesto en numeral 84.2 del artículo 84 de la Ley N°32069, Ley General de Contrataciones Públicas. En caso de duda o falta de acuerdo, el arbitraje es resuelto por árbitro único, a no ser que la complejidad o cuantía de las controversias justifique la conformación de un tribunal arbitral, lo cual es determinado por las partes o conforme al Reglamento de la institución arbitral competente. En el caso de los arbitrajes ad hoc, la controversia es resuelta por arbitro único.

CLÁUSULA VIGÉSIMA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA PRIMERA: NOTIFICACIONES DURANTE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen vía notarial conforme la Décimo Tercera Disposición Complementaria Transitoria del Reglamento:

DOMICILIO DE LA ENTIDAD CONTRATANTE: [.....]

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince días calendario.

El CONTRATISTA señala el siguiente correo electrónico para efectos de las notificaciones que se realicen durante la ejecución del presente contrato, que no se realicen a través del SEACE de la Pladicop:

CORREO ELECTRÓNICO CONTRATISTA: [CONSIGNAR EL CORREO ELECTRÓNICO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del correo electrónico aquí declarado debe ser comunicada a la entidad contratante, formalmente y por escrito, con una anticipación no menor de cinco días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [**CONSIGNAR FECHA**].

"LA ENTIDAD CONTRATANTE"

"EL CONTRATISTA"

Advertencia

La entidad contratante suscribe el contrato mediante firma digital, en caso de que el postor adjudicado con la buena pro cuente con certificado digital emitido por una entidad de certificación, de acuerdo con la normativa de la materia. Excepcionalmente, la entidad contratante con el debido sustento puede proceder a la firma del contrato mediante medios manuales, de acuerdo con el numeral 87.3 del artículo 87 del Reglamento,

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], postor y/o representante Legal de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**], identificado con [**CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD**] N° [**CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], con poder inscrito en la localidad de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s):		
MYPE[16]	SI ( )	NO ( )	
Correo electrónico:			

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de negociación regulado en el artículo 132 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 91 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra, de ser el caso.

Asimismo, me comprometo a remitir la confirmación de recepción del correo electrónico, en el plazo máximo de dos días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal, según corresponda

Advertencia
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la entidad contratante reciba acuse de recepción.

[16] Esta información será verificada por la entidad contratante en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link: http://www2.trabajo.gob.pe/servicios-en-linea-2-2/ y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 114, del Reglamento.

Advertencia
Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR EN CONSORCIO

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], representante común del consorcio [**CONSIGNAR EL NOMBRE DEL CONSORCIO**], identificado con [**CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1			
Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s) :		
MYPE[17]	SI ( )	NO ( )	
Correo electrónico:			

Datos del consorciado 2			
Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s) :		
MYPE[18]	SI ( )	NO ( )	
Correo electrónico:			

Datos del consorciado 3			
Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s) :		
MYPE[19]	SI ( )	NO ( )	
Correo electrónico:			

Autorización de notificación por correo electrónico:

Correo electrónico común del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

[17] Esta información será verificada por la entidad contratante en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link: http://www2.trabajo.gob.pe/servicios-en-linea-2-2/ y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 114, del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

[18] Ibidem.

[19] Ibidem.

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de negociación regulado en el artículo 132 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 91 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra, de ser el caso.

Asimismo, me comprometo a remitir la confirmación de recepción del correo electrónico, en el plazo máximo de dos días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, nombres y apellidos del representante común del consorcio

Advertencia
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la entidad contratante reciba acuse de recepción.

ANEXO N° 2

PACTO DE INTEGRIDAD[20]

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que suscribe, [……..], postor y/o representante legal de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], con poder inscrito en la localidad de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**] en la Ficha Nº [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**] Asiento Nº [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, en su calidad de proveedor en el ámbito de aplicación de la normativa de contratación pública, **suscribo el presente Pacto de Integridad** bajo los siguientes términos y condiciones:

PRIMERO: Declaro, bajo juramento:

1. Que conozco los impedimentos para ser participante, postor, contratista o subcontratista, establecidos en el artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.
2. Que los recursos que componen mi patrimonio o el patrimonio de la persona jurídica a la que represento no provienen de lavado de activos, narcotráfico, minería ilegal, financiamiento del terrorismo, y/o de cualquier actividad ilícita.
3. Que conozco la obligación de denunciar cualquier acto de corrupción cometido por los actores del proceso de contratación, así como las medidas de protección que le asisten a los denunciantes[21]; además de las consecuencias administrativas y legales que de estos se derivan.
4. Que conozco el alcance de la Ley N° 28024, Ley que regula la gestión de intereses en la administración pública y su reglamento, aprobado por Decreto Supremo N° 120-2019-PCM, así como el marco de aplicación de la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público, y su reglamento aprobado por Decreto Supremo N° 082-2023-PCM[22].
5. Que conozco el alcance de la cláusula anticorrupción y antisoborno de los contratos suscritos en el marco del proceso de contratación y las consecuencias derivadas de su incumplimiento[23].

SEGUNDO: Dentro de ese marco, asumo los siguientes compromisos:

[20] De conformidad con el literal b del numeral 69.1 del artículo 69 y el numeral 57 del Anexo I Definiciones del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[21] Decreto Legislativo N° 1327, Decreto Legislativo que establece medidas de protección para el denunciante de actos de corrupción y sanciona las denuncias realizadas de mala fe, y su Reglamento aprobado por Decreto Supremo N.° 010-2017-JUS, modificado por Decreto Supremo N° 002-2020-JUS, en concordancia con la Directiva N° 002-2023-PCM-SIP: Directiva para la gestión de denuncias y solicitudes de medidas de protección al denunciante de actos de corrupción recibidas a través de la plataforma digital única de denuncias del ciudadano, aprobada por aprobada por Resolución de Secretaría de Integridad Pública N° 005-2023-PCM-SIP.

[22] Reglamento de la Ley N° 31564:
Artículo 24.- Inhabilitación de ex funcionarios, ex servidores públicos, empresas e instituciones privadas
El incumplimiento de los impedimentos señalados en el numeral 4.2 del artículo 4 de la Ley por parte de las personas, las empresas e instituciones privadas involucradas en dicho incumplimiento, es sancionado con la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad, sin perjuicio de las acciones civiles y penales a que hubiera lugar conforme al numeral 7.7 del artículo 7 de la Ley. En caso de ex funcionarios y ex servidores públicos se aplica el procedimiento administrativo disciplinario sujeto a la Ley N° 30057, Ley del Servicio Civil o normas específicas. (…)

[23] Conforme a lo establecido en el artículo 68 de la Ley General de Contrataciones Públicas, así como en el artículo 274 numeral d), de su Reglamento:
Artículo 68. Resolución del contrato
68.1. Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:
d) Por incumplimiento de la cláusula anticorrupción.
Artículo 274. Causales de exclusión de proveedores adjudicatarios de los catálogos electrónicos de acuerdo marco
Un proveedor adjudicatario es excluido de los Catálogos Electrónicos de Acuerdo Marco, en los siguientes casos:
d) Por incumplimiento de la cláusula anticorrupción y antisoborno.

1. Mantener una conducta proba e íntegra en todas las actividades del proceso de contratación, lo que supone actuar con honestidad y veracidad, sin cometer actos ilícitos, directa o indirectamente, así como respetar la libertad de concurrencia y las condiciones de competencia efectiva en el proceso de contratación y abstenerme de realizar prácticas que la restrinjan o afecten.

   [**Solo para personas jurídicas**]
   Lo anterior se hace extensivo, para conocimiento, a los socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a la persona jurídica que represento.

2. Abstenerme de ofrecer, dar o prometer regalos, cortesías, invitaciones, donativos u otros beneficios similares, a funcionarios o servidores públicos de la dependencia encargada de las contrataciones, actores del proceso de contratación y personal de la entidad contratante.

3. Denunciar ante las autoridades competentes, de manera oportuna, los actos de corrupción, inconducta funcional, conflicto de intereses u otro de naturaleza similar, respecto de lo cual tuviera conocimiento en el marco del proceso de contratación (https://denuncias.servicios.gob.pe/).

4. Facilitar las acciones o mecanismos implementados por la entidad pública responsable del proceso de contratación para fortalecer la transparencia, promover la lucha contra la corrupción y fomentar la rendición de cuentas.

TERCERO: Este pacto de integridad tiene vigencia desde el momento de su suscripción hasta la culminación de la fase de selección[24]; y, en caso de resultar adjudicado con la buena pro, este mantiene su vigencia hasta la finalización del proceso de contratación.

CUARTO: Para efectos de salvaguardar el contenido del Pacto de Integridad frente a eventuales incumplimientos de los compromisos asumidos, me someto a las acciones de debida diligencia, supervisión, fiscalización posterior, iniciativas de veeduría autorizadas por la entidad contratante u otros que correspondan; así como a las responsabilidades administrativas, civiles y/o penales que se deriven de estos, conforme al marco legal vigente.

En señal de conformidad, suscribo el presente pacto de integridad, a los ( ) días del mes ( ) de 20( ), manifestando que la información declarada se sujeta al principio de presunción de veracidad, conforme a lo dispuesto en el artículo IV del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General[25].

Firma

N° de DNI:

[24] **Artículo 92. Culminación de la fase de selección,** del Decreto Supremo N°009-2025-EF:
La fase de selección culmina cuando: a) Se perfecciona el contrato, b) Se cancela el procedimiento de selección, c) Se deja sin efecto el otorgamiento de la buena pro por causa imputable a la entidad contratante, d) No se perfeccione el contrato por los supuestos establecidos en el artículo 91.

[25] *1.7 Principio de Presunción de Veracidad. - En la tramitación del procedimiento administrativo, se presume que los documentos y declaraciones formulados por los administrados en la forma prescrita por esta Ley, responden a la verdad de los hechos que ellos afirman. Esta presunción admite prueba en contrario.*

ANEXO Nº 3[26]

DECLARACIÓN JURADA

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

Mediante el presente el suscrito, postor y/o representante legal de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**], declaro bajo juramento:

i. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.

ii. Conocer las sanciones contenidas en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado mediante Decreto Supremo N° 009-2025-EF, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iii. 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.

iv. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.

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

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

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal, según corresponda

Advertencia
En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

[26] Artículo 69 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

ANEXO Nº 4

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

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por los artículos 88 y 89 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF, bajo las siguientes condiciones:

a) Integrantes del consorcio
   1. [**NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1**].
   2. [**NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2**].

b) Designamos a [**CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN**], identificado con [**CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [**CONSIGNAR NOMBRE DE LA ENTIDAD**].

   Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....] y nuestro correo electrónico común: […….], al cual se notificaran todas las comunicaciones dirigidas al Consorcio durante el procedimiento de selección hasta la suscripción del contrato.

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

   1. OBLIGACIONES DE **[NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1]** [%][27]

      [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

   2. OBLIGACIONES DE **[NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]** [%][28]

      [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

[27] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[28] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

TOTAL OBLIGACIONES	100%[29]

[CONSIGNAR CIUDAD Y FECHA]

……

Consorciado 1
Nombres, apellidos y firma del consorciado 1
o de su representante legal
tipo y N° de documento de identidad

……..

Consorciado 2
Nombres, apellidos y firma del consorciado 2
o de su representante legal
tipo y N° de documento de identidad

……..

Consorciado 3
Nombres, apellidos y firma del consorciado 3
o de su Representante Legal
Tipo y N° de Documento de Identidad

[29] Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

Advertencia

El Anexo N° 5 únicamente es presentado por los postores que, si bien son parientes de los impedidos referidos en el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, no le son aplicables los impedimentos en razón de parentesco del inciso 2 del citado numeral, debido a que cumplen alguna de las siguientes condiciones: i) Han suscrito un contrato derivado de un procedimiento de selección competitivo o no competitivo o, ii) han ejecutado cuatro contratos menores en el mismo tipo de objeto al que postula. Para el caso de bienes y obras, el pariente debe haber ejecutado los contratos dentro de los dos años previos a la convocatoria del procedimiento de selección, contratación directa o a la adjudicación de un contrato menor.

ANEXO Nº 5[30]
DECLARACIÓN JURADA DE DESAFECTACIÓN DE IMPEDIMENTO

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]
Presente.-

El que suscribe, [……..], postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**] Asiento Nº [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA**], **declaro que tengo los siguientes parientes[31], los cuales cuentan con impedimento de carácter personal[32] de conformidad con el numeral 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, de acuerdo a lo siguiente:**

[NOMBRE DEL PARIENTE 1] con DNI **[……..]** con CARGO **[……]** en la ENTIDAD **[……..]** que a la fecha de la presente declaración cuenta con impedimento de carácter personal de Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, según corresponda]** de conformidad con el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069 Ley General de Contrataciones Públicas.

[NOMBRE DEL PARIENTE 2] con DNI **[……..]** con cargo **[……]** en la entidad **[……..]** que a la fecha de la presente declaración cuenta con impedimento de carácter personal de Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, SEGÚN CORRESPONDA]** de conformidad con el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069 Ley General de Contrataciones Públicas.

Sin perjuicio de ello, **DECLARO BAJO JURAMENTO** lo siguiente:

Me encuentro exceptuado del impedimento por razón de parentesco, en razón de [INDICAR SUPUESTO: HABER EJECUTADO UN CONTRATO DERIVADO DE UN PROCEDIMIENTO DE SELECCIÓN COMPETITIVO O NO COMPETITIVO / HABER EJECUTADO CUATRO CONTRATOS MENORES EN EL MISMO TIPO DE OBJETO AL QUE POSTULA] dentro de los dos años previos a la convocatoria del procedimiento de selección, contratación directa o a la adjudicación de un contrato menor] conforme al inciso 2 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, lo cual acredito documentalmente para la presentación de ofertas, de conformidad con el numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones del Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[30] Numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[31] Se entiende pariente a aquellos hasta el segundo grado de consanguinidad y segundo de afinidad, lo que incluye al cónyuge, al conviviente, y al progenitor del hijo.

[32] Aplicables a autoridades, funcionarios o servidores públicos de acuerdo con lo que señala la Ley N° 32069, Ley General de Contrataciones Públicas.

[CONSIGNAR EL DETALLE DE LOS DOCUMENTOS CORRESPONDIENTES]

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, nombres y apellidos del postor o representante legal, según corresponda

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta en en **[CONSIGNAR LA MONEDA DE LA CONVOCATORIA]** e incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluyen en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Advertencia

- *En caso de que el postor reduzca su oferta, según lo previsto en el artículo 132 del Reglamento, debe presentar nuevamente este Anexo.*
- *El postor que goce de alguna exoneración legal debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*
  "Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".
- *En caso de divergencia entre el precio de la oferta en dígitos y en letras, prevalece este último.*

ANEXO N° 8

DECLARACIÓN JURADA DE PRESENTACIÓN DE FIDEICOMISO COMO GARANTÍA DE FIEL CUMPLIMIENTO DEL CONTRATO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], postor adjudicado y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado **con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD]** N° **[CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, declaro bajo juramento su compromiso de presentar la constitución de un fideicomiso como mecanismo de garantía de fiel cumplimiento del contrato, en un plazo no mayor a veinte días hábiles contabilizados desde el día siguiente de perfeccionado el mismo, en el marco de los artículos 116 y 138 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Advertencia
El fideicomiso es aplicable, de acuerdo con los artículos 116 y 138 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF, siempre que el plazo de la ejecución contractual sea mayor a noventa días calendario.

ANEXO Nº 9

AUTORIZACIÓN DE NOTIFICACIONES DURANTE LA EJECUCIÓN CONTRACTUAL MEDIANTE CORREO ELECTRÓNICO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], postor adjudicado y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA],** identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD]** N° **[CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD],** autorizo que durante la ejecución del contrato se me notifique al correo electrónico **[INDICAR EL CORREO ELECTRÓNICO].**

[CONSIGNAR CIUDAD Y FECHA]

…….
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Advertencia
La notificación de la decisión de la entidad contratante respecto a solicitudes presentadas durante la ejecución contractual se efectúa por correo electrónico, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.

ANEXO N° 10[33]

ELECCIÓN DE INSTITUCIÓN ARBITRAL

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], postor adjudicado y/o representante legal de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA],** identificado con [**CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, elijo la institución arbitral del listado proporcionado por la entidad contratante:

[INDICAR LA RAZON SOCIAL DE LA INSTITUCIÓN ARBITRAL ELEGIDA, DE ACUERDO AL LISTADO DEL NUMERAL 3.3 DEL CAPÍTULO III DE LA SECCIÓN ESPECÍFICA DE LAS BASES]

[CONSIGNAR CIUDAD Y FECHA]

…….
Firma, nombres y apellidos del postor o
representante legal o común, según corresponda

s y reducciones, de ser el caso.

[33] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

[33] Consignar en la moneda establecida en las bases.

ANEXO Nº 11

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD*:*

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [34]	FECHA DE LA CONFORMIDAD DE SER EL CASO[35]	EXPERIENCIA PROVENIENTE DE:	MONEDA	IMPORTE[36]	TIPO DE CAMBIO VENTA[37]	MONTO FACTURADO ACUMULADO[38]
1										
2										
3										
4										
5										
6										
7										
8										
9										

[34] Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

[35] **Únicamente**, cuando la fecha del perfeccionamiento del contrato sea previa a los diez años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

[36] Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

[37] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

[38] Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [34]	FECHA DE LA CONFORMIDAD DE SER EL CASO[35]	EXPERIENCIA PROVENIENTE DE:	MONEDA	IMPORTE[36]	TIPO DE CAMBIO VENTA[37]	MONTO FACTURADO ACUMULADO[38]
10										
…										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o
representante legal o común, según corresponda

Advertencia

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal considerando que ambas constituyen la misma persona jurídica conforme a lo previsto en el artículo 396 de la Ley N° 26887, Ley General de Sociedades, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Del mismo modo, en aplicación de lo previsto en la mencionada Ley, en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante puede acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante puede acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante puede emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe.

ANEXO Nº 12

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de selección la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de **[CONSIGNAR EL PLAZO OFERTADO. EN CASO DE LA MODALIDAD DE LLAVE EN MANO O LLAVE EN MANO CON MANTENIMIENTO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].**

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, nombres y apellidos del postor o
representante legal o común, según corresponda

ANEXO Nº 14

DECLARACIÓN JURADA

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]
Presente.-

Mediante el presente el suscrito, postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA],** declaro que la experiencia que acredito de la **empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA]** como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 72.3 del artículo 72 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal, según corresponda

Advertencia
A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones Públicas con Sanción Vigente en http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados. *También le asiste dicha facultad a la dependencia encargada de las contrataciones o al órgano de la entidad contratante al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.*

ANEXO Nº 15
DECLARACIÓN JURADA DE ACTUALIZACIÓN DE DESAFECTACIÓN DE IMPEDIMENTO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
DEPENDENCIA ENCARGADA DE LAS CONTRATACIONES
LICITACIÓN PÚBLICA PARA BIENES Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]
PROCEDIMIENTO]
Presente.-

El que suscribe, [……..], postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la localidad de El que suscribe, [……..], postor y/o representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** Asiento Nº **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, **declaro que tengo los siguientes parientes[39], los cuales cuentan con impedimento de carácter personal[40] de conformidad con el numeral 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, de acuerdo a lo siguiente:**

NOMBRE DEL PARIENTE 1 [……] con DNI [……..] con CARGO [……..….] en la ENTIDAD [……..] que a la fecha de la presente declaración es un impedido de carácter personal del Tipo [CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, según corresponda].

NOMBRE DEL PARIENTE 2 [……] con DNI [……..…..] con CARGO [……..……..….] en la ENTIDAD [……...] que a la fecha de la presente declaración es un impedido de carácter personal del Tipo [CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, según corresponda] .

Sin perjuicio de ello, **DECLARO BAJO JURAMENTO** lo siguiente:

A la fecha me encuentro exceptuado del impedimento por razón de parentesco, en razón de [INDICAR SUPUESTO: HABER SUSCRITO UN CONTRATO DERIVADO DE UN PROCEDIMIENTO DE SELECCIÓN COMPETITIVO O NO COMPETITIVO / HABER EJECUTADO CUATRO CONTRATOS MENORES EN EL MISMO TIPO DE OBJETO AL QUE POSTULA] dentro de los dos años previos a la convocatoria del procedimiento de selección, contratación directa o a la adjudicación de un contrato menor] conforme al inciso 2 del numeral 30.1 del artículo 30 de la Ley N° 32069[41], Ley General de Contrataciones Públicas, lo cual acredito de conformidad con el numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones del Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

En ese sentido, mediante el presente cumplo con presentar la acreditación documental correspondiente:

[CONSIGNAR EL DETALLE DE LOS DOCUMENTOS CORRESPONDIENTES]

[39] Se entiende pariente a aquellos hasta el segundo grado de consanguinidad y segundo de afinidad, lo que incluye al cónyuge, al conviviente, y al progenitor del hijo.
[40] Aplicables a autoridades, funcionarios o servidores públicos de acuerdo con lo que señala la Ley N° 32069, Ley General de Contrataciones Públicas.
[41] Conforme el numeral 2 “Impedimentos en razón del parentesco” del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal, según corresponda

ANEXO Nº 16

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC

Mediante el presente el suscrito, postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Importante
• *Para asignar la bonificación, la Dependencia Encargada de las Contrataciones o los evaluadores, según corresponda, verifica la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link **http://www2.trabajo.gob.pe/servicios-en-linea-2-2/**.*
• *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.*

ANEXO Nº 17[42]

DECLARACIÓN JURADA SOBRE INAPLICACIÓN DEL IMPEDIMENTO TIPO 4.D DEL INCISO 4 DEL NUMERAL 30.1 DEL ARTÍCULO 30 DE LA LEY N° 32069 REFERIDO A LA INSCRIPCIÓN EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS – REDAM
(Documento a presentar para el perfeccionamiento del contrato en caso de proveedores con procesos de alimentos en ejecución de sentencia)

Señores
EVALUADORES
LICITACIÓN PÚBLICA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que suscribe, [……..], postor y/o apoderado de **[CONSIGNAR EL NOMBRE DE LA PERSONA NATURAL QUE OTORGA EL PODER, DE SER EL CASO]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD**], con poder inscrito en la localidad de **[CONSIGNAR EN CASO DE CONTAR CON APODERADO]** en la Ficha Nº **[CONSIGNAR EN CASO DE CONTAR CON APODERADO**] Asiento Nº [**CONSIGNAR EN CASO DE CONTAR CON APODERADO**], **DECLARO BAJO JURAMENTO** que no me resulta aplicable el impedimento Tipo 4.D del inciso 4 del numeral 30.1 del artículo 30 de la Ley, referido a las personas inscritas en el Registro de Deudores Alimentarios Morosos del Poder Judicial (Redam), considerando lo siguiente**:**

[EL PROVEEDOR DEBE CONSIGNARSÓLO UNA DE LAS OPCIONES QUE SE ESTABLECEN A CONTINUACIÓN, SEGÚN SEA EL CASO]:

- Que, se ha remitido el/la **[CONSIGNAR LA DENOMINACIÓN EXACTA DEL DOCUMENTO REMITIDO POR EL PROVEEDOR AL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS]** con fecha de recepción **[CONSIGNAR FECHA DE RECEPCIÓN]** dirigido/a al **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS QUE CORRESPONDA],** mediante el cual se informó la cancelación de la deuda alimentaria derivada del proceso de alimentos seguido por **[CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS]**, para lo cual me sujeto al principio de presunción de veracidad. Se adjunta el cargo de recepción del indicado documento.

- Que, sí me encuentro en el registro de deudores alimentario moroso, por lo que; autorizo se me descuente del pago que me corresponde como contraprestación del contrato derivado del presente procedimiento de selección, el monto de la pensión mensual fijada en el proceso de alimentos seguido por **[CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS]** ante el **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO CORRESPONDIENTE]**, para lo cual adjunto:

  a) La sentencia emitida por el **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS QUE CORRESPONDA]** en el trámite del proceso de alimentos seguido en el expediente **[CONSIGNAR EL NÚMERO DE EXPEDIENTE JUDICIAL]**

[42] De conformidad con lo previsto en el numeral 39.2 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

b) La información complementaria solicitada por la entidad contratante para realizar el descuento, la que comprende lo siguiente: **[LA ENTIDAD CONTRATANTE DEBE CONSIGNAR LA INFORMACIÓN QUE REQUIERA DEL PROVEEDOR PARA HACER EFECTIVO EL DESCUENTO]**

[CONSIGNAR CIUDAD Y FECHA]

…….....

Firma, nombres y apellidos del postor o apoderado, según corresponda

ANEXO N° 18

ELECCIÓN DEL CENTRO DE JUNTA DE PREVENCIÓN Y RESOLUCIÓN DE DISPUTAS

(Documento a presentar para el perfeccionamiento del contrato)

Señores
EVALUADORES
LICITACIÓN PÚBLICA ABREVIADA PARA BIENES Nº 001-2025-OC-UNJFSC
Presente.-

El que se suscribe, [……..], postor adjudicado y/o representante legal de [**CONSIGNAR EN CASO DE SER PERSONA JURÍDICA],** identificado con [**CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, elijo el Centro de Administración de la Junta de Resolución de Disputas del listado proporcionado por la entidad contratante:

[INDICAR LA RAZÓN SOCIAL DEL CENTRO DE ADMINISTRACIÓN DE JUNTA DE RESOLUCIÓN DE DISPUTAS ELEGIDA, DE ACUERDO A LA NOTA IMPORTANTE PARA LA ENTIDAD, INDICADA EN NUMERAL 3.3 DEL CAPÍTULO III DE LA SECCIÓN ESPECÍFICA DE LAS BASES]

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, nombres y apellidos del postor o apoderado, según corresponda