CONCURSO PÚBLICO
Nº 004-2024-CS/MIDIS

CONTRATACIÓN DE
SERVICIO DE INTERNET DEDICADO PARA EL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL

PAC - ID 20

DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios previstos en la Ley de Contrataciones del Estado.

En este contexto, se encuentran obligados a prestar su colaboración al OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información referida a las contrataciones del Estado que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 30225, Ley de Contrataciones del Estado, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley de Contrataciones del Estado aprobado por Decreto Supremo N° 344-2018-EF.

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

1.2. CONVOCATORIA

Se realiza a través de su publicación en el SEACE de conformidad con lo señalado en el artículo 54 del Reglamento, en la fecha señalada en el calendario del procedimiento de selección, debiendo adjuntar las bases y resumen ejecutivo.

1.3. REGISTRO DE PARTICIPANTES

El registro de participantes se realiza conforme al artículo 55 del Reglamento. En el caso de un consorcio, basta que se registre uno (1) de sus integrantes.

Importante

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.rnp.gob.pe.*
- *Los proveedores que deseen registrar su participación deben ingresar al SEACE utilizando su Certificado SEACE (usuario y contraseña). Asimismo, deben observar las instrucciones señaladas en el documento de orientación "Guía para el registro de participantes electrónico" publicado en https://www2.seace.gob.pe/.*
- *En caso los proveedores no cuenten con inscripción vigente en el RNP y/o se encuentren inhabilitados o suspendidos para ser participantes, postores y/o contratistas, el SEACE restringirá su registro, quedando a potestad de estos intentar nuevamente registrar su participación en el procedimiento de selección en cualquier otro momento, dentro del plazo establecido para dicha etapa, siempre que haya obtenido la vigencia de su inscripción o quedado sin efecto la sanción que le impuso el Tribunal de Contrataciones del Estado.*

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento.

Importante

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.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en los numerales 72.4 y 72.5 del artículo 72 del Reglamento.

Importante

- *No se absolverán consultas y observaciones a las bases que se presenten en forma física.*
- *Cuando exista divergencia entre lo indicado en el pliego de absolución de consultas y observaciones y la integración de bases, prevalece lo absuelto en el referido pliego; sin perjuicio, del deslinde de responsabilidades correspondiente*

1.6. ELEVACIÓN AL OSCE DEL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRACIÓN DE BASES

Los cuestionamientos al pliego de absolución de consultas y observaciones así como a las bases integradas por supuestas vulneraciones a la normativa de contrataciones, a los principios que rigen la contratación pública u otra normativa que tenga relación con el objeto de la contratación, pueden ser elevados al OSCE de acuerdo a lo indicado en los numerales del 72.8 al 72.11 del artículo 72 del Reglamento.

La solicitud de elevación para emisión de Pronunciamiento se presenta ante la Entidad, la cual debe remitir al OSCE el expediente completo, de acuerdo a lo señalado en el artículo 124 del TUO de la Ley 27444, aprobado por Decreto Supremo N° 004-2019-JUS, al día hábil siguiente de recibida dicha solicitud.

Advertencia

La solicitud de elevación al OSCE de los cuestionamientos al pliego de absolución de consultas y observaciones, así como a las Bases integradas, se realiza de manera electrónica a través del SEACE, a partir de la oportunidad en que establezca el OSCE mediante comunicado.

Importante

Constituye infracción pasible de sanción según lo previsto en el literal n) del numeral 50.1 del artículo 50 de la Ley, presentar cuestionamientos maliciosos o manifiestamente infundados al pliego de absolución de consultas y/u observaciones.

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 del Reglamento.

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[1]). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

- *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.*
- *En caso la información contenida en los documentos escaneados que conforman la oferta no*

[1] Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales

coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.

- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

El participante presentará su oferta de manera electrónica a través del SEACE, desde las 00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

El participante debe verificar antes de su envío, bajo su responsabilidad, que el archivo pueda ser descargado y su contenido sea legible.

Importante
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.

En la apertura electrónica de la oferta, el comité de selección, verifica la presentación de lo exigido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos y condiciones de los Términos de Referencia, detallados en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.9. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el artículo 74 del Reglamento.

El desempate mediante sorteo se realiza de manera electrónica a través del SEACE.

1.10. CALIFICACIÓN DE OFERTAS

La calificación de las ofertas se realiza conforme a lo establecido en los numerales 75.1 y 75.2 del artículo 75 del Reglamento.

1.11. SUBSANACIÓN DE LAS OFERTAS

La subsanación de las ofertas se sujeta a lo establecido en el artículo 60 del Reglamento. El plazo que se otorgue para la subsanación no puede ser inferior a un (1) día hábil.

La solicitud de subsanación se realiza de manera electrónica a través del SEACE y será remitida al correo electrónico consignado por el postor al momento de realizar su inscripción en el RNP, siendo su responsabilidad el permanente seguimiento de las notificaciones a dicho correo. La notificación de la solicitud se entiende efectuada el día de su envío al correo electrónico.

La presentación de las subsanaciones se realiza a través del SEACE. No se tomará en cuenta la subsanación que se presente en físico a la Entidad.

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas

que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los resultados de la admisión, no admisión, evaluación, calificación, descalificación, rechazo y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los ocho (8) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

En caso que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.

El consentimiento del otorgamiento de la buena pro se publica en el SEACE al día hábil siguiente de producido.

Importante
Una vez consentido el otorgamiento de la buena pro, el órgano encargado de las contrataciones o el órgano de la Entidad al que se haya asignado tal función realiza la verificación de la oferta presentada por el postor ganador de la buena pro conforme lo establecido en el numeral 64.6 del artículo 64 del Reglamento.

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. 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.

El recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

Los actos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por el Titular de la Entidad que afecten la continuidad de este, se impugnan ante el Tribunal de Contrataciones del Estado.

Importante
• *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.* *Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.* • *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 deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.* • *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los ocho (8) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

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, se interpone dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

Los plazos y el procedimiento para perfeccionar el contrato se realiza conforme a lo indicado en el artículo 141 del Reglamento.

Para perfeccionar el contrato, el postor ganador de la buena pro debe presentar los documentos señalados en el artículo 139 del Reglamento y los previstos en la sección específica de las bases.

3.2. GARANTÍAS

Las garantías que deben otorgar los postores y/o contratistas, según corresponda, son las de fiel cumplimiento del contrato y por los adelantos.

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

Como requisito indispensable para perfeccionar el contrato, el postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del mismo por una suma equivalente al diez por ciento (10%) del monto del contrato original. Esta se mantiene vigente hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesoria, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

En caso se haya previsto en la sección específica de las bases la entrega de adelantos, el contratista debe presentar una garantía emitida por idéntico monto conforme a lo estipulado en el artículo 153 del Reglamento.

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, 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.

Importante
Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro y/o contratista cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. 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).* *2. 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.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *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.* *De otro lado, 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 el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).* *Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

3.4. EJECUCIÓN DE GARANTÍAS

La Entidad puede solicitar la ejecución de las garantías conforme a los supuestos contemplados en el artículo 155 del Reglamento.

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

3.6.2. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada en el numeral precedente, según lo previsto en el artículo 163 del Reglamento y lo indicado en la sección específica de las bases.

Estos dos tipos de penalidades se calculan en forma independiente y pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

3.7. INCUMPLIMIENTO DEL CONTRATO

Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

3.8. PAGOS

El pago se realiza después de ejecutada la respectiva prestación, pudiendo contemplarse pagos a cuenta, según la forma establecida en la sección específica de las bases o en el contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción, 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 quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

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

Advertencia
En caso de retraso en los pagos a cuenta o pago final por parte de la Entidad, salvo que se deba a caso fortuito o fuerza mayor, esta reconoce al contratista los intereses legales correspondientes, de conformidad con el artículo 39 de la Ley y 171 del Reglamento, debiendo repetir contra los responsables de la demora injustificada.

3.9. DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente 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 DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO A LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL
RUC Nº	:	20545565359
Domicilio legal	:	Av. Paseo de la República N° 3101 – San Isidro
Teléfono:	:	631-8000 Anexo 1534
Correo electrónico:	:	arojas@midis.gob.pe fchoquehuayta@midis.gob.pe wgarcia@midis.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del **servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social**.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante el FORMATO 02 Nº 026-2024-MIDIS/SG/OGA el 06 de junio de 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos ordinarios. Certificación de Crédito Presupuestario N° 1225 y Previsión Presupuestal para los años fiscales 2025 y 2026 otorgados mediante Memorando N° D000692-2024-MIDIS-OP del 31 de mayo de 2024.

Importante
La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de suma alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. DISTRIBUCIÓN DE LA BUENA PRO

No aplica.

1.7. ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el Capítulo III de la presente sección de las bases.

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de veinticuatro (24) meses contados desde el día siguiente de firmada el "acta de inicio del servicio", el acta de inicio del servicio deberá firmarse por el contratista y la Oficina General de Tecnología de Información del MIDIS luego que se concluya con la implementación y se suscriba el acta de implementación.

El plazo de implementación del servicio será de sesenta (60) días calendario como máximo, contabilizados a partir del día siguiente de la firma del contrato, este período comprende, la instalación y puesta en producción completa del servicio, en concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar el monto de S/ 5.00 (Cinco con 00/100 Soles) en la Cuenta N° 068-376386 del Banco de la Nación; posterior a ello la entrega se efectuará en la Oficina de Abastecimiento del MIDIS sito en Av. Paseo de La República 3101, San Isidro, piso 12, de lunes a viernes en el horario de 8:30 a.m. a 5:30 p.m.

Importante
El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.

1.10. BASE LEGAL

- Ley N° 31953, Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 31954, Ley de Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 28411, Ley General del Sistema Nacional de Presupuesto.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N° 082-2019-EF.
- Reglamento de la Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 344-2018-EF y modificado por Decretos Supremos N°377-2019-EF, N° 168-2020-EF, N° 250-2020-EF, N° 162-2021-EF, N° 234-2022-EF, N° 308-2022-EF y N° 051-2024-EF.
- Resolución Ministerial N° 073-2021-MIDIS, que aprueba el Texto Integrado actualizado del Reglamento de Organización y Funciones del Ministerio de Desarrollo e Inclusión Social.
- Resolución Ministerial N° 074-2022-MIDIS, que aprueba el Manual N° 003-2022-MIDIS, "Manual del Sistema Integrado de Gestión del Ministerio de Desarrollo e Inclusión Social", numeral 5.2, Política del Sistema Integrado de Gestión (SIG).
- Resolución Ministerial Nº D000001-2024-MIDIS, sobre delegación de facultades y atribuciones en diversos funcionarios del MIDIS, durante el Año Fiscal 2024.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante
De conformidad con la vigesimosegunda Disposición Complementaria Final del Reglamento, en caso la Entidad (Ministerios y sus organismos públicos, programas o proyectos adscritos) haya difundido el requerimiento a través del SEACE siguiendo el procedimiento establecido en dicha disposición, no procede formular consultas u observaciones al requerimiento.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos2, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. (**Anexo N° 1)**

b) 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, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

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 es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[3] 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.

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo N° 2)**

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

e) Documento en el cual se indique la marca y modelo del equipo ofertado, según lo

[2] La omisión del índice no determina la no admisión de la oferta.

[3] Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace https://www.gobiernodigital.gob.pe/interoperabilidad/

indicado en el literal v. del numeral 4.1 de los términos de referencia.

f) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[4]

g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio 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 5**)

h) El precio de la oferta en soles. Adjuntar obligatoriamente el **Anexo Nº 6.**

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

Importante
• *El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.*
• *En caso de requerir estructura de costos o análisis de precios, esta se presenta para el perfeccionamiento del contrato.*

2.2.1.2. 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 3.2 del Capítulo III de la presente sección de las bases.

Advertencia
El comité de selección no podrá 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".

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato.
b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior. (**Anexo N° 7**).
d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
e) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

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 es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[5] y

[4] En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

[5] Para mayor información de las Entidades usuarias de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace https://www.gobiernodigital.gob.pe/interoperabilidad/

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).

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [6] (**Anexo N° 10**).
h) Detalle de los precios unitarios del precio ofertado[7].
i) Copia simple de la documentación para acreditar el perfil y la experiencia de los especialistas en seguridad, de acuerdo al numeral 9 de los Términos de Referencia.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del 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 podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2 opción consulta de empresas acreditadas en el REMYPE.*

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[8].*

- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

---

[6] En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

[7] Incluir solo en caso de la contratación bajo el sistema a suma alzada.

[8] Según lo previsto en la Opinión N° 009-2016/DTN.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida, dirigida a la Oficina de Abastecimiento, en la Mesa de Partes del Ministerio de Desarrollo e Inclusión Social, sito en Av. Paseo de la República N° 3101, San Isidro – Primer piso en el horario de 08:30 a.m. a 05:00 p.m. o a través de la Mesa de Partes Virtual del Ministerio de Desarrollo e Inclusión Social ingresando al link correspondiente:

https://mesapartesvirtual.midis.gob.pe/appmesapartesenlinea/inicio.

Importante
En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de servicios, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

Asimismo, adicional al envío de la documentación y, en caso el postor ganador de la buena pro presente garantía de fiel cumplimiento del contrato, deberá remitir el original a la Mesa de Partes del Ministerio de Desarrollo e Inclusión Social, en la misma fecha en que se envía el resto de la documentación.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos periódicos, en forma mensual por un periodo de 24 meses en armadas iguales.

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

- Informe del funcionario responsable de la Oficina General de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada, acompañado del informe técnico emitido por el especialista a cargo de la supervisión del servicio.
- Comprobante de pago.
- Entregables correspondientes, según lo indicado en el numeral 7 de los términos de referencia.

La documentación indicada se debe presentar en la Mesa de Partes del Ministerio de Desarrollo e Inclusión Social, sito en Av. Paseo de la República N° 3101, San Isidro – Primer piso en el horario de 08:30 a.m. a 05:00 p.m. o a través de la Mesa de Partes Virtual del Ministerio de Desarrollo e Inclusión Social ingresando al link correspondiente:

https://mesapartesvirtual.midis.gob.pe/appmesapartesenlinea/inicio.

CAPÍTULO III
REQUERIMIENTO

Importante

De conformidad con el numeral 29.8 del artículo 29 del Reglamento, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

3.1. TERMINOS DE REFERENCIA

SERVICIO DE INTERNET DEDICADO PARA EL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL

Órgano y/o Unidad Orgánica:	Oficina General de Tecnologías de la Información
Actividad del POI	0088314. Ejecución de Acciones de Tecnología de la Información
Meta Presupuestal	0014
Denominación de la Contratación:	Servicio de Internet Dedicado para el Ministerio de Desarrollo e Inclusión Social

1. ANTECEDENTES

El Ministerio de Desarrollo e Inclusión Social (MIDIS) creado mediante la Ley 29792 de octubre de 2011 articula la política social. Es su competencia formular, dirigir, coordinar, ejecutar, supervisar y evaluar la política nacional y sectorial en materia de desarrollo e inclusión social encaminadas a reducir la pobreza, las desigualdades, vulnerabilidades y riesgos sociales en aquellas brechas que no pueden ser cubiertas por la política social. Por ello, se tiene la necesidad de contar con una adecuada comunicación tanto interna como externa.

2. FINALIDAD PÚBLICA

- Tener acceso a todo servicio de información disponible en Internet que sea de pertinencia para el MIDIS, con fines de búsqueda, difusión y consulta de información de interés institucional.
- Brindar a los usuarios del MIDIS las facilidades técnicas para comunicarse o compartir información mediante los servicios disponibles en Internet.
- Compartir información, conocimiento, formas de colaboración y cooperación entre diversas comunidades interconectadas mediante Internet, lo que optimizará las coordinaciones y el desarrollo de las actividades del MIDIS, apoyando así al cumplimiento de las metas de desarrollo e inclusión social en el Perú.

3. OBJETIVO

Contratar el servicio de internet para el Ministerio de Desarrollo e Inclusión Social, el cual permita que los usuarios puedan acceder a los servicios tanto a los usuarios internos y externos del MIDIS.

4. DESCRIPCIÓN DEL SERVICIO

Los requerimientos mínimos que deberá cumplir el proveedor para implementar el servicio de Internet dedicado para el MIDIS deberán ser los siguientes:

Descripción	Medida
Servicio de internet dedicado para el MIDIS	Servicio

4.1. CARACTERÍSTICAS DEL SERVICIO DE INTERNET

a. El backbone deberá contar con las siguientes características:
   - Ser de fibra óptica a nivel metropolitano.
   - Contar como mínimo con dos (02) salidas internacionales del tipo TIER-1, ambas redundadas y con una capacidad agregada de 20Gbps
   - Tener conexión propia al NAP Perú con una capacidad mínima de 2x100Gbps.

b. Se deberá brindar un enlace de Internet con una capacidad mínima de 500Mbps y en alta disponibilidad (activo – pasivo) para lo cual debe considerarse: □ Ambos enlaces serán de la misma capacidad.
   Ruta de fibra principal y ruta de fibra de contingencia (independientes)
   Nodo de red principal y nodo de red contingencia
   - Cada enlace debe contar con su propio equipo router
   - Debe incluirse 02 equipos switches para la configuración del escenario

c. El postor deberá incluir dos (02) routers en la sede principal del MIDIS.
d. La administración de los routers será ejecutada por el PROVEEDOR a un primer nivel, brindando al MIDIS acceso autenticado (usuario y pasword) a nivel de lectura.
e. Los router deberán estar en capacidad de aumentar el ancho de banda contratado hasta en un 50% de la capacidad contratada a solicitud del MIDIS cuando lo requiera, este incremento será realizado mediante una adenda al contrato.
f. Los router debe de ser un appliance de propósito dedicado cuya función principal es la de enrutar tráfico (capa 3 del modelo OSI), por lo que no se aceptarán dispositivos cómo: firewalls, UTM, NGFW o NGIPS.
g. Los routers deberá tener como mínimo tres (03) interfaces Ethernet 100/1000.
h. Los router deberán tener la capacidad mínima de memoria de RAM/FLASH 4GB/4GB.
i. Los router deberá soportar los siguientes protocolos de ruteo: RIPv2, OSPF y BGP como mínimo.
j. Los router deberá soportar el protocolo 802.3ad LACP (o similar).
k. Los router deberá soportar los protocolos: 802.1p CoS Priorización de tráfico y 802.1q trunking.
l. Garantía del Fabricante por los Routers a través de RMA durante el periodo de contrato. El postor deberá contar con una unidad similar o superior para reemplazo en modalidad 24x7x4; (anexo 3).
m. El PROVEEDOR deberá garantizar la confidencialidad e integridad de la información desde la puerta de enlace del MIDIS hasta la salida internacional, de acuerdo con el TUO de la Ley General de Telecomunicaciones vigente respecto al secreto de las telecomunicaciones.
n. Todo el equipamiento para implementar por el proveedor deberá soportar protocolo IPv6 el cual será implementando por la entidad en forma progresiva con la asistencia del proveedor del servicio.
o. El PROVEEDOR deberá brindar sesenta (60) direcciones IP públicas IPv4 del mismo segmento, adicionalmente se requieren como mínimo con quince (15) direcciones IPv6, se precisa que estas IPs son dedicadas para publicación, en el caso del broadcast, red y de configuración el proveedor deberá considerar las IPs necesarias para este fin.
p. El PROVEEDOR deberá brindar el servicio DNS para publicaciones, como mínimo deberá contar dos (02) direcciones IP o nombres para resolución de nombres DNS.
q. El PROVEEDOR deberá ofrecer sin costo adicional, una página de gestión vía WEB SEGURA, la cual permita acceso autenticado (usuario / password) para el monitoreo y supervisión del estado y uso del enlace contratado, así como permitir el reporte de estadísticas de uso, que contemple el volumen de tráfico mensual, semanal, anual, etc. así como el tipo de tráfico según protocolos básicos (HTTP, SMTP, FTP, SSL, etc.) de comunicación la cual podrá estar en la nube del proveedor y mantendrá un historia de 2 meses. Debe permitirse la descarga de reportes en formato pdf y/o CSV a demanda directamente por la Entidad.
r. El PROVEEDOR sólo será responsable de las configuraciones de los equipos que formen parte de la solución ofertada, siendo la ENTIDAD la responsable de las configuraciones de sus equipos.
s. Los equipos de seguridad de la información (Firewalls) y los equipos de comunicación que sean utilizados en la implementación del servicio deberán ser nuevos y/o contar con vigencia tecnológica de los fabricantes (contar con soporte del fabricante durante la vigencia del contrato). Una vez finalizado el plazo contractual, el contratista procederá con el recojo del total de los equipos que le hayan sido entregados como parte del servicio, sin más desgaste que el de su uso normal y diligente, para lo cual la entidad brindará las facilidades correspondientes. La entidad velará por el uso correcto de los equipos; sin embargo, en caso ocurran daños irreparables en los equipos, el contratista gestionará con el fabricante o una empresa autorizada

por el fabricante, evaluar previamente si la responsabilidad deberá recaer sobre el contratista o sobre la Entidad.

t. El PROVEEDOR deberá identificar y etiquetar todos los equipos de comunicación y medios físicos de conexión que utilizará para brindar el servicio dentro de las instalaciones del MIDIS. Este etiquetado deberá estar descrito en un diagrama en el cual se identifique todos los componentes que participan en la implementación del servicio. Este requerimiento será realizado y presentado en la etapa de instalación de los servicios.

u. Todos los equipos, materiales de cableado, accesorios, obras civiles dentro y fuera de las instalaciones del MIDIS y otro componente a ser instalado para la provisión del servicio deberán ser brindados por el PROVEEDOR sin costo adicional para el MIDIS, quien brindará las siguientes facilidades:
   - El proveedor deberá proveer el cable de conexión hacia el switch de propiedad del MIDIS el cual cuenta con soporte vigente y las interfaces físicas o puertos necesarios (1Geth RJ45). El swtich estará en otro gabinete diferente al que se instalará los equipos del servicio de internet y deberán estar a una distancia no mayor dos metros.
   - Energía eléctrica estabilizada mediante dos líneas independientes y tomas de corriente con terminación tipo C13 para cada uno de los equipos.
   - Sistema de Aire acondicionado.
   - Se brindará espació dentro de un (01) gabinete y 14 RU como máximo en el gabinete, dentro del centro de datos, el cual tiene sistema de aterramiento, switches y cableado LAN.
   - Se brindará todas las facilidades de acceso, teniendo a su cargo la responsabilidad la ENTIDAD de gestionar las autorizaciones de ingreso necesarias, de desocupar los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación, respecto a la parte externa el PROVEEDOR deberá gestionar los permisos ante las entidades correspondientes.

v. Se deberá indicar en su oferta la marca y modelo del equipo ofertado.

4.2. CARACTERÍSTICAS DE MITIGACIÓN DDoS

a. El proveedor deberá incluir un equipo para DDoS, en condición de alquiler para lo cual deberá instalar un equipo basado en un appliance en hardware de propósito dedicado, por lo que no se aceptarán dispositivos que dependan de información de estado de la conexión para poder mitigar, cómo: firewalls, sistemas de prevención y detección de intrusos (IDS/IPS) ADC y las variantes o combinaciones como UTM, NGFW, NGIPS. A continuación, se detallan las funcionalidades de la solución

b. El appliance debe contar con fuentes de alimentación AC redundantes y las interfaces necesarias para poder monitorear y proteger contra ataques de DDoS, por lo menos para los dos enlaces de internet solicitados.

c. El sistema debe de tener embebido bypass físico en cada interface de protección sea de cobre o de fibra óptica, para garantizar alta disponibilidad y deberá activarse en los siguientes casos: Perdida de energía eléctrica, falla lógica en la interface de control, pérdida de conectividad con la tarjeta madre del dispositivo, colapso del sistema operativo.

d. El sistema debe venir licenciado para proteger el ancho de banda a ofrecer no debe tener un límite de sesiones o conexiones concurrentes para el tráfico total, ni para el tráfico atacante ni para el tráfico legítimo que atraviesa el dispositivo y permitir el aumento de su rendimiento hasta 10 Gbps a través de cambios de licenciamiento, sin la necesidad de reemplazar el equipo.

e. Debe ser una solución dedicada a la protección en sitio en línea contra ataques de denegación de servicios distribuidos (DDoS) desde capas 3 a 7 (Incluyendo http y/o https), que permita ser gestionada sin la necesidad de componentes adicionales gracias a su interfaz gráfica embebida, de manera que minimice los puntos de falla.

f. El sistema debe proporcionar un panel de estado de dispositivo que incluya información sobre el Top de alertas activas, top de grupos de protección, total del tráfico permitido y bloqueado a través del dispositivo, estado de la CPU y memoria de sistema.

g. La solución deberá de ser capaz de analizar los servicios del cliente y predecir los siguientes valores para las protecciones basadas en tasas: pps (Paquetes por segundo), bps (bits por segundo) para bloqueos por umbrales, tasa de peticiones http por segundo, tasa de objetos http por segundo, tasa de peticiones DNS, tasa de respuestas NXDomain, tasa de mensajes SIP, tasa de bits por segundo y paquetes por segundo para ICMP, UDP y fragmentación.

h. El sistema debe de soportar una configuración en donde no reenvíe el tráfico entre los puertos de protección al operar en modo espejo, SPAN, o tap de red, para evitar la inyección de tráfico duplicado. La configuración para "nunca reenviar el tráfico" no deberá de poder ser modificada en el flujo de trabajo de la interfaz de usuario normal.

i. La solución debe hacer una efectiva mitigación de los principales tipos de ataques de denegación de servicio, entre ellos:
   - Ataques de inundación por avalancha TCP/UDP/HTTP
   - Protección contra botnets;
     Protección ataques volumétricos tipo Chargen.
     Protección contra hacktivistas;
   - Protección de comportamiento de host;
   - Anti-suplantación ;
   - Filtrado configurable de expresiones de avalancha;
   - Filtrado basado en expresiones de carga;
   - Listas negras y blancas permanentes y dinámicas;
   - Creación de formas de tráfico;
   - Varias protecciones para HTTP, HTTPS, DNS;
   - Protección para SIP: requerimiento de límite de velocidad SIP.
   - Ataques a la pila TCP; ataques de fragmentación; ataques de conexión.
   - Mitigación de ataques basados en aplicación / Web Servers - HTTP: incorporar firmas AIF, expresión regular de carga útil.
   - Mitigación de ataques basados en aplicación / Servidores SIP: SIP malformado, requerimiento de límite de velocidad SIP.
   - Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico.
   - Mitigación de ataques basados en aplicación / Basados en Volumen: Chargen, Fragmentación ICMP/UDP/TCP, NTP reflexion, SSDP.
   - Además, la solución debe proteger contra ataques de Botnets controladas manual o automáticamente.

j. El sistema debe de poder bloquear tráfico de amenazas y ataques en forma saliente desde la red protegida hacia Internet, por medio de inteligencia que reconozca amenazas de Emails, Reputación de DDoS, Malware, servidores de command y control, así como por medio de la definición de filtros y umbrales (por ejemplo, umbrales de tasas por segundo de tráfico DNS), y bloqueo de tráfico HTTP malformado.

k. El sistema deberá de proteger contra amenazas que atenten contra el protocolo TLS y debe hacer cumplir el uso correcto del protocolo SSL/TLS y bloquear las solicitudes SSL / TLS malformadas.

l. El sistema debe detectar encabezados SSL / TLS extendidos y debe detectar ataques de agotamiento de conexión y ataques basados en tasas contra SSL/TLS.

m. El sistema debe soportar la prevención de ataques SSL / TLS para tráfico TLS HTTPS y no HTTPS.

n. Como mínimo el sistema debe ser capaz de bloquear paquetes inválidos realizando comprobaciones para encabezados IP malformados, fragmentos incompletos, checksum IP erróneos, fragmentos duplicados, fragmentos muy largos, paquetes pequeños, paquetes TCP pequeños, paquetes UDP pequeños, paquetes ICMP pequeños, checksums TCP/UDP erróneos, banderas TCP inválidas, números ACK inválidos. Además, debe proporcionar estadísticas para los paquetes descartados.

o. La solución debe permitir al usuario bloquear desde la Interfaz gráfica de usuario (GUI) tráfico discriminado por país de origen y seleccionar si se bloqueará para todo el tráfico hacia los recursos protegidos o para un recurso protegido en particular.

p. La solución debe permitir colocar host en listas blancas y negras de manera global o de manera individual por cada recurso ó grupo de protección definido, además debe permitir filtrar ataques por país de origen, expresiones regulares en el payload del paquete, la cabera http o incluso permitir/denegar tráfico que coincida con un filtro.

q. Las contramedidas/protecciones de la solución deben ser flexibles y no requerir detener/reiniciar el servicio para poder ser activadas/desactivadas o modificadas, deben permitir el cambio en los parámetros de protección mientras se encuentran en ejecución y visualizar el efecto de estos cambios sobre el tráfico hacia los recursos protegidos a través de su interfaz gráfica embebida.

r. El sistema debe de ser capaz de bloquear hosts que exceden un umbral configurable para el número total de operaciones http por segundo, por grupo protegido.

s. El sistema debe permitir la configuración de protecciones predefinidas asociadas con servicios específicos, como Web, DNS, VoIP o un servidor genérico.

t. La solución deberá de proporcionar una línea base en bps y pps para la tasa de tráfico, tráfico bloqueado y botnets

u. La solución debe ser flexible de manera que permita al operador ingresar sus propias expresiones regulares o filtros a través de la interfaz gráfica, para filtrar por Payload, cabecera http, request/cabecera DNS
v. El sistema debe utilizar un protocolo de señalización propietario del fabricante para realizar la solicitud de mitigación ascendente hacia soluciones antiDDoS en la nube (ISP o nube del fabricante). Esto será usado y contratado en caso se requiera mitigar ataques de DDoS desde los peer de las salidas internacionales, en caso exista un ataque colateral de otro cliente y que está afectando al MIDIS
w. El sistema debe proporcionar estadísticas detalladas y gráficos para cada protección, mostrando su impacto en el tráfico durante los últimos 5 minutos, 1 hora, 24 horas, 7 días o un intervalo personalizado especificado.
x. Las estadísticas detalladas y gráficos para cada grupo de protección para los servidores, deben incluir información sobre el tráfico total, tráfico total permitido y bloqueado, número de hosts bloqueados, estadísticas sobre cada tipo de prevención que ha tenido impacto en el tráfico, información de ubicación IP, distribución de protocolos, distribución de servicios y estadísticas principales de hosts bloqueados para el periodo de tiempo seleccionado.
y. La solución debe tener una herramienta de análisis de paquetes integrada en la Interfaz gráfica de usuario (GUI) tipo wireshark, que permita desplegar filtros por host de origen/destino, país, servicio, interfaz, grupo de protección; para los paquetes capturados, tráfico pasado, tráfico descartado y que entregue información sobre la política que ocasionó el descarte.
z. El sistema debe de ser capaz de regularmente activar las nuevas técnicas de defensa actualizando las firmas que serán mantenidas por el equipo de investigación del fabricante 24x7.
aa. Garantía del fabricante por el hardware a través de RMA durante el periodo de contrato.
bb. Se debe proteger de ataques encriptados sin necesidad de desencriptar o sin violar la privacidad de las conexiones.
cc. La solución debe soportar multi-tenat, con la finalidad de separar el uso a nivel de zonas o tráfico

4.3. CARACTERÍSTICAS DE ADMINISTRACIÓN DE ANCHO DE BANDA

a. Un equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras. Deberá ser una solución integral de hardware y software por parte del fabricante y de propósito dedicado.
b. El equipo deberá soportar un rango de operación hasta 1Gbps, pero el licenciamiento será para el ancho de banda mínimo de 500Mbps
c. El equipo deberá incluir al menos 2 pares de interfaces bypass de 1GE las cuales podrán ser RJ45 u ópticas.
d. Capacidad de realizar políticas de control de tráfico a través de horarios definidos.
e. Las políticas o reglas de control de ancho de banda deben permitir: priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo ancho de banda permitido.
f. Flexibilidad en la priorización, definición de políticas de QoS, capacidad de compartir tráfico y asignación de ancho de banda.
g. Capacidad de detectar y clasificar tráfico por direcciones o rangos de direcciones IP, usuarios, servicio (aplicación) y VLAN.
h. Soportar como mínimo 600,000 flujos concurrentes
i. Soportar como mínimo 850,000 paquetes por segundo.
j. Permitir la generación de políticas de control de ancho de banda para el tráfico entrante y saliente de manera independiente para las aplicaciones y usuarios, deben permitir: priorización de tráfico (al menos 4 niveles de prioridades), definir un mínimo ancho de banda garantizado y un máximo ancho de banda permitido
k. La solución deberá integrarse con los Directorios Activos (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios.
l. Deberá permitir la creación de los siguientes reportes históricos basados en gráficos para un periodo de tiempo configurable: □ Tráfico de descarga y de subida
   - Top 10 de Host con mayor consumo
   - Top 10 de Usuarios con mayor consumo (cuando se haya integrado con el Directorio Activo).
   - Top 10 de Aplicaciones con mayor consumo
   - Top 10 de Aplicaciones más populares (muestra qué aplicaciones que tienen mayor número de usuarios sin importar su consumo de ancho de banda)
m. Deberá contar con el análisis histórico de distintas métricas del desempeño a nivel de un usuario utilizando una aplicación específica, mínimamente:

- Troughput (In / Out)
- Bytes transmitidos (In / Out)
- Número de Sesiones activas y nuevas sesiones por segundo
- Número de paquetes descartados y paquetes descartados por segundo

n. La administración y manejo de reportes puede realizarse desde el mismo equipo o un equipo externo instalado en la Entidad.
o. La solución debe presentar reportes de gráficos lineales (históricos y de tiempo real con actualizaciones cada segundo) de las políticas de optimización, de al menos las siguientes métricas:
   - Número de flujos activos
   - Bytes transmitidos de descarga y subida
   - Utilización de ancho de banda (troughput) de descarga y subida
   - Paquetes descartados de descarga y subida
   - Congestión de la política de descarga y subida

4.4. CARACTERÍSTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.4.1. DESCRIPCIÓN

a. Implementación de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
b. La solución tiene que ser ofrecida en alta disponibilidad (2 appliances).
c. La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
d. El equipo ofertado no debe tener anuncio de end-of-life o end-of-sale o end-of-support por parte del fabricante al momento de la presentación de la oferta.
e. Los equipos NGFW deberán tener garantía y soporte vigente de fabrica durante la vigencia del contrato.
f. Se deberá proporcionar dos (02) cuentas de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías.
g. Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, firmware cerca a la obsolescencia, expiración de licencias.

4.4.2. CAPACIDAD

a. Throughput de Next Generation Firewall de 4.2 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
b. Throughput de Prevención de Amenazas de 1.8/2.3 Gbps (Http o mixapp) medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
c. El equipo debe soportar como mínimo 390,000 sesiones simultaneas y 63,000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte.
d. Almacenamiento interno de 120 GB o superior.
e. Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red
f. Deberá contar con una interfaz 10/100/1000 out-of-band y un puerto de consola RJ45

4.4.3. CAPACIDADES DE NETWORKING

a. El equipo debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, enrutamiento dinámico (RIPv2, BGP y OSPFv2).
b. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
c. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
d. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
e. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
f. Soportar IPv6 en modos Activo/Activo y Activo/Pasivo.

4.4.4. ALTA DISPONIBILIDAD

a. Soporte de configuración en alta disponibilidad activo/pasivo y activo/activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
b. La configuración en alta disponibilidad debe sincronizar: Sesiones; certificados de descifrado, configuraciones, incluyendo, más no limitado a políticas de firewall, NAT, QoS y objetos de red.
c. Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
d. Debe permitir cifrar la comunicación entre dos firewall de HA durante la sincronización de las configuraciones.

4.4.5. FUNCIONALIDADES DE FIREWALL

a. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
b. Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
c. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
d. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.

4.4.6. DESCIFRADO DE TRÁFICO SSL/TLS

a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
d. Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
e. Sebe permitir el descifrado selectivo de categorías de URLs, por ejemplo debe ser capaz de especificar el no descifrado de paginas con contenido sensible, mientras forzar el descifrado de paginas de clasificación de riesgo alto o medio

4.4.7. CONTROL DE APLICACIONES

a. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
b. Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
c. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
d. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas

también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.

e. Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5104, mms-ics, rockwell, siemens, entre otros.
f. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
g. Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.
h. Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

4.4.8. PROTECCION DoS

a. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
b. La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS
c. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo

4.4.9. PREVENCION DE AMENAZAS CONOCIDAS

a. Los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
b. Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos
c. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
d. Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
e. Los eventos deben identificar el país que origino la amenaza.
f. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

4.4.10. ANALISIS DE MALWARE DE DÍA CERO

a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
b. La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye firmas o prefiltros).
c. Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines)
d. Deberá ser una plataforma del mismo fabricante.
e. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.
f. El NGFW deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.
g. Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, ISO 27001, ISO 27017 e ISO 27018.
h. Deberá contar con una acreditación alineada con estándares HIPAA, GDPR y PCI.

i. Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
j. El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB, tanto en IPv4 como en IPv6.
k. Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
l. Permitir la subida de archivos al sandbox de forma manual y vía API.
m. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
n. En caso de tratarse de una plataforma de Sandboxing On-premise con equipos dedicados, deberá cumplir adicionalmente con los siguientes requerimientos:
   - Deberá ser desplegado en Alta Disponibilidad (02 equipos)
   - Deberá ser capaz de analizar al menos 4200 archivos por hora, sin sufrir degradación ni encolamiento y haciendo uso completo de técnicas de emulación y análisis dinámico (es decir, sin considerar Firmas, Prefiltros, ni Machine Learning).
   - Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows, MacOS, Linux y Android.
   - Debe admitir topologías de implementación en modo sniffer o en linea (in-line)

4.4.11. FILTRO DE CONTENIDO WEB

a. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
b. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
c. Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
d. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.
e. Debe permitir la creación de categorías personalizadas.
f. Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
g. Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
h. Debe permitir la customización de la página de bloqueo.
i. Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
j. Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.

4.4.12. PROTECCION AVANZADA DE DNS

a. La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.
b. El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros como minimo.
c. La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
d. Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA
e. Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
f. Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización.

4.4.13. IDENTIFICACION DE USUARIOS

a. Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active

Directory, E- Novell Directory, Exchange y base de datos local.
b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
d. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
e. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.

4.4.14. QOS

a. Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.
b. El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.

4.4.15. VPN

a. Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
b. La VPN IPSec debe soportar como mínimo:
c. DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
d. Autenticación MD5, SHA-1, SHA-2;
e. Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
f. Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
g. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
h. Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
i. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
j. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
k. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
l. Antes del usuario se autentique en la estación;
m. Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
n. Bajo demanda del usuario;
o. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, Windows 11 y MacOS X.
p. Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
q. Mínimo 700 licencias para usuarios conectados
r. Mínimo 2 licencias para equipos moviles

4.4.16. CONSOLA DE ADMINISTRACION Y MONITOREO

a. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante instalado en la Sede de MIDIS (on-premise). En caso de ser un appliance independiente deberá estar en alta disponibilidad (02 equipos) y doble fuente de alimentación.
b. Permitir exportar las reglas de seguridad en formato CSV y PDF
c. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
d. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
e. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.

f. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
g. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
h. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
i. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración
j. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
k. Debe permitir el estándar OpenConfig (OC) para automatizar las tareas de configuración del NGFW.

4.5. CARACTERÍSTICAS DE PROTECCIÓN DE APLICACIONES WEB

4.5.1. CARACTERISTICAS GENERALES

a. La solución debe de ser del tipo appliance físico
b. El equipo (appliance físico) debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web, así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.
c. Deberá brindar al menos 250Mbps como Throughput protegido.
d. Deberá disponer de al menos 480GB de almacenamiento interno.
e. Deberá de soportar al menos 4 puertos GE RJ45 opcional 4 puertos SFP GE.
f. Garantía del Fabricante por el HW a través de RMA durante el periodo de contrato, se deberá

4.5.2. NETWORKING Y GESTIÓN

a. La solución debe permitir implementación en modo Proxy Transparente y Proxy Reverso.
b. Soportar direccionamiento IPv4 y IPv6
c. El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y/o también por CLI (interface de línea de comando), accediendo localmente al equipo por puerto de consola, o remotamente vía SSH.
d. Debe de soportar administración basada en interface web HTTPS.
e. Debe de soportar administración basada en interface de línea de comando vía SSH.
f. Debe de proveer, en la interfaz de gestión o CLI, las siguientes informaciones del sistema: consumo de CPU y una gráfica que muestre los últimos 30 días.
g. Debe de ser posible visualizar en la interfaz de gestión o CLI la información de consumo de memoria.
h. Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI).
i. Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog.
j. La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG.
k. La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías.
l. La solución debe tener datos analíticos, siendo posible visualizar el total de ataques de cada país de origen.
m. Debe soportar RESTFUL API para gestión de la configuración.

4.5.3. AUTENTICACION Y CERTIFICACION

a. Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP y/o HTTPS.
b. Debe tener base local para almacenamiento y autenticación de los usuarios.
c. La solución debe tener la capacidad de autenticar usuarios en bases externas remotas como mínimo LDAP, RADIUS.
d. La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM como mínimo.

e. Debe soportar CAPTCHA cuando detecte una IP y país sospechoso.
f. Debe soportar autenticación de doble factor.
g. La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP.
h. El equipo debe de tener certificación FCC Class A part 15, VCCI, ETSI EN 300 386 V1.6.1, EN 61000-3-2:2014.

4.5.4. WAF

a. Debe tener soporte nativo de HTTP/2.
b. Deberá soportar interoperabilidad con OpenAPI 3.0
c. Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de reputación IP, la cual se debe actualizar automáticamente y de manera periódica que permita bloquear tráfico desde y hacia direcciones IP en categorías como: Scanners, Exploits Windows, Denial of Service, Proxy de Phishing, Botnets, Proxy anónimos.
d. Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje automático de máquina y creación de políticas de seguridad con generador de políticas incorporado en tiempo real.
e. Deberá minimizar la ocurrencia de Falsos Positivos y/o falsos negativos utilizando Inteligencia Artificial u otra técnica.
f. Tener mecanismo de aprendizaje automático capaz de validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto.
g. Tener la capacidad de creación de firmas o eventos de ataques customizables.
h. Tener la capacidad de protección contra ataques tipo:
   - Botnet
   - Browser Exploit Against SSL/TLS (BEAST) o Web Scrapping
   - Acceso por fuerza bruta
   - Clickjacking
   - Cambios de cookie
   - Zero Day Attacks o Forceful Browsing
   - Cross Site Request Forgery (CSRF)
   - Cross site scripting (XSS)
   - Denial of Service (DoS)
   - Local File inclusion (FLI)
   - Remote File Inclusion (RFI)
   - Low-rate DoS o XML bombs/DoS
   - Slowloris
   - Malformed o alteración de parámetros XML
   - SYN flood
   - Parameter and HPP Tampering
   - Manipulación de campos ocultos
   - Manipulación de campos ocultos
   - Fallas de secuencias de comandos de sitio
   - Desbordamientos de búfer
   - Control de acceso roto
   - Autenticación rota y gestión de sesión
   - Manejo inadecuado de errores
i. El WAF debe admitir la funcionalidad de forward proxy SSL para crear dinámicamente un certificado SSL de servidor único antes de iniciar la conexión del lado del servidor.
j. Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection).
k. Tener la capacidad de configurar protección del tipo TCP SYN flood-style o HTTP Get Flood para prevención o mitigación de DoS.
l. Permitir configurar reglas de bloqueo a métodos HTTP no deseados.
m. Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país.
n. Debe soportar crear políticas de geolocalización, permitiendo que el tráfico de determinado país sea bloqueado.
o. Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen.
p. Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataque detectado por la solución.

q. Debe permitir añadir, automática o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
r. Tener la capacidad de validar que las credenciales que usan los usuarios para acceder a algún sistema no sean credenciales robadas o permita el cifrado dinámico de las credenciales al momento de ser tecleadas en el browser..
s. Tener la capacidad de protección o prevención contra pérdida de datos salientes o pérdida de información (DLP).
t. Tener la funcionalidad de proteger el website contra acciones de defacement contra modificaciones de la web.
u. Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo o soportar la comprobación de virus en las cargas de archivos HTTP y los archivos adjuntos SOAP.
v. Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado.
w. La solución debe de ser capaz de funcionar como terminador de sesión SSL.
x. La solución debe tener la capacidad de almacenar certificados digitales de CA's.
y. La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL.
z. La solución debe contener las firmas de bot conocidos o admitir la función Anti-bot que detecte bots y clasifique clientes, identificando el comportamiento humano.
aa. La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automáticamente.
bb. La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores como minimo.
cc. La solución debe permitir la customización o reenvío de solicitaciones y respuestas HTTP, como minimo.
dd. La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
ee. La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP. ff. La solución debe tener la capacidad de proteger contra modificación de campos ocultos.
gg. Permitir que se configuren firmas customizadas de ataques, a través de expresiones regulares
hh. La solución debe permitir la integración con scanners de vulnerabilidades de terceros, tales como IBM AppScan, WhiteHat, Qualys, HP WebInspect.s etc., para proveer parches virtuales.
ii. Debe generar perfil de protección automáticamente o manual a partir de reporte generado por scanner de vulnerabilidad de terceros.
jj. Debe permitir programar la verificación de vulnerabilidades. kk. La solüción debe generar un reporte de análisis de vulnerabilidades.
ll. Soportar redirección y/o reescritura de requisiciones y respuestas HTTP. mm. Permitir redirección de requisiciones HTTP para HTTPS.
nn. Permitir reescribir la línea URL del encabezado de una requisición HTTP oo. Permitir reescribir el campo HOST del encabezado de una requisición HTTP. pp. Permitir redirigir requisiciones para otro website.
qq. Permitir añadir o interpretar el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso
rr. La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como Form Post, Protocol Token Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación ss. Tener capacidad de caching para aceleración web, o compresión de software. tt. Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes. uu. El WAF debe soportar Camellia Ciphers Suites
vv. El WAF debe ser capaz de proporcionar un aprendizaje anómalo de la integridad del cliente si se basa en el navegador en comparación con la herramienta de ataque web automatizada (es decir, Bot)
ww. El WAF debe admitir las siguientes técnicas de detección evasiva
- Decodificación de URL
- Terminación de cadena de bytes nulos
- Rutas de autorreferencia (es decir, uso de /./ y equivalentes codificados)
- Referencias de ruta (es decir, uso de /../ y equivalentes codificados)
- Caso mixto
- Uso excesivo de espacios en blanco
- Eliminación de comentarios (por ejemplo, convertir BORRAR / ** / DE a BORRAR DE)

- Conversión de caracteres de barra invertida (compatibles con Windows) en caracteres de barra diagonal.
- Conversión de codificación Unicode específica de IIS
- Decodificación de entidades HTML (por ejemplo, c, & quot ;, & # xAA;)
- Técnicas de modelo de seguridad negativa.

4.5.5. BALANCEO DE CARGA

a. La solución debe incluir la funcionalidad de balanceo de carga entre servidores web.
b. Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS.
c. Soportar balanceo / distribución de tráfico y enrutar el contenido hacia distintos servidores web
d. Soportar los siguientes algoritmos de balanceo de carga de servidores.
   - Round Robin
   - Weighted Least ConnectionRound Robin
   - Least Connection
   - Ratio Least Connections
e. Implementar Cache de Contenido o Compresión para HTTP y aceleración Web,
f. La solución debe de ser capaz de balancear las nuevas sesiones, implementando persistencia basada en:
   - Cookie Persistente
   - Destination Address
   - Host
   - Source Address

4.6. CARACTERÍSTICAS DE INFRAESTRUCTURA DE CONTINGENCIA

a. Debe provisionarse de recursos de cómputo desde una nube privada alojada en el Centro de Datos del Contratista en territorio nacional, los recursos deben estar activos y disponibles durante toda la vigencia del contrato.
b. El Centro de Datos puede ser propio y/o tercerizado y/o subcontratado y contar con certificación TIER III Uptime Institute o ANSI/TIA Rated 3, en Diseño y/o Construcción y/o Operación.
c. Los recursos para provisionarse se muestran en la Tabla N°1. En el caso de las licencias serán provistos por la entidad.
d. Debe considerarse un servicio de internet de 50Mbps de ancho de banda y 8 IPv4 asociado a las VM. Este ancho de banda será usado para publicar servicios.
e. Debe considerarse la conexión entre el Centro de Datos y la Sede Principal del MIDIS mediante un enlace de datos de 50Mbps. El enlace de datos solicitado es para el acceso del MIDIS a los recursos de cómputo
f. La configuración, y puesta en marcha de los sistemas operativos será realizado por el MIDIS.
g. El licenciamiento que se usara en los recursos de cómputo ofertados será provistos por el MIDIS.
h. La instalación, configuración y puesta en marcha de las aplicaciones son responsabilidad del MIDIS.
i. El requerimiento del MIDIS es solo por los siguientes servicios de infraestructura: vCPU, Memoria RAM y disco (GB), en una nube privada. Durante toda la vigencia del contrato.

La entidad será la responsable de la administración y del correcto funcionamiento de los sistemas operativos y de las aplicaciones que se encuentren configurados en los recursos de computo durante toda la duración del contrato.

SOFTWARE	VCPU	MEMORIA RAM (GB)	DISCO (GB)
Windows Server 2019 + SQL 2019 Standard	8	192	4096
Windows Server 2019 + SQL 2019 Standard	4	32	2048
Red Hat Enterprise Linux	4	32	6144
Red Hat Enterprise Linux	4	32	300
TOTAL	**22**	**288**	**12,588**

4.7. CARACTERISTICAS SOBRE LA ATENCION DE AVERÍAS

a. El Proveedor deberá contar con un NOC (Centro de Operaciones Networking) propio (no rentado a terceros) y un SOC (seguridad Security Operation Center) podrá ser propio o rentado a terceros, para brindar gestión, administración y seguridad de los servicios que contrata el MIDIS. El servicio de soporte deberá ser permanente bajo la modalidad 24 horas x 7 días durante el periodo del servicio y contar con un sistema de gestión adecuado para reportar fallas y atenciones mediante este centro de operaciones, via correo electrónico y un numero 0800 gratuito.
b. El SOC propio o tercerizado del postor deberá contar con una solución SIEM (Security Information and Event Management) y deberá cumplir con las siguientes características mínimas:
   - El servicio de monitoreo y colección de eventos debe estar integrada, licenciada y alojada en el centro de datos propio o tercerizado o en la nube del fabricante.
   - Se deberá ofertar soluciones del tipo SIEM (Security Information and Event Management) que incluya el motor de correlación en tiempo real que permita gestionar de forma proactiva e instantánea las amenazas de seguridad.
   - Deberá estar licenciado (base de datos, Windows Workstation, Windows Server y/o dispositivos, según corresponda) mientras dure el servicio para al menos 10 dispositivos, entre ellos los equipos Firewall a proponer, routers y equipos críticos del cliente con sistema operativo Windows Server.
   - Deberá estar activo el servicio por el tiempo que dure el contrato.
   - Deberá recolectar, analizar, buscar, generar informes y archivar todos los eventos desde una ubicación central.
   - Deberá automatizar la respuesta a incidentes mediante el uso de workflow de incidentes.
   - Almacenar grandes cantidades de información sin requierir un storage adicional, para lo cual deberá soportar una ratio de compresión mínima de 20 a 1, la Entidad determinará las fuentes (equipos) que enviarán datos a la plataforma SIEM y el Contratista será responsable de garantizar el almacenamiento de esta información.
   - Deberá contar con reglas predefinidas de correlación para una gestión proactiva de las amenazas.
   - Deberá señalar o marcar los intentos de acceso, amenazas internas, violaciones de políticas, etc. sin intervención manual.
   - Generar informe forense de red como actividad de usuarios, auditoria de sistemas y reportes de conformidad con normativas regulatorias de seguridad.
   - Generar informes predefinidos de conformidad para cumplir con normativas PCI, HIPAA, GLBA, SOX, GDPR, IS027001:2013
   - Búsqueda de cualquier término, así como un grupo de campos pre-indexados, y detecte rápidamente anomalías en la red: configuraciones erróneas, virus, actividades de usuarios, errores del sistema / de las aplicaciones, etc.
   - Permitir coleccionar y analizar todos los eventos sobre las actividades de los usuarios privilegiados.
   - Las alertas automáticas permitan recibir en tiempo real notificaciones vía correo electrónico y ejecución de scripts para remediación. La ejecución de scripts serán realizados en coordinación con la entidad para la ejecución de la remediación.
   - Debe incluir el módulo de Threat Hunting que permita la búsqueda proactiva de amenazas avanzadas de seguridad y la inspección de actividades maliciosas en la red e incluir un sistema de respuesta ante eventos en tiempo real que lo alerte acerca de eventos críticos y ofrecer opciones de búsqueda de logs para detectar y detener actividades maliciosas.
   - Debe incluir el módulo Threat Intelligence y Threat Analytics o el modulo NTA o que permita mitigar posibles ataques y detectar actividades sospechosas en la red. El cual podrá realizarse mediante una plataforma de terceros.
   - Se deberá brindar informes mensuales de los módulos de Threat Hunting en donde el postor deberá concertar una reunión virtual y/o presencial para exponer los eventos de seguridad encontrados en los equipamientos de Firewall.
c. Disponibilidad mensual de 99.90% como mínimo para el servicio de Internet, se entenderá por avería a una interrupción parcial o total del servicio.
d. Se deberá entender que toda interrupción parcial del servicio está determinada como mínimo por los siguientes incidentes: pérdida de paquetes hasta la salida internacional 10% en una hora, una latencia superior a los 90ms hasta la salida internacional.
e. Se entenderá por tiempo de respuesta a cualquier llamada en que se solicite a atender una falla por perdida del servicio hasta la asignación de un ticket de atención.

f. Se entenderá por Tiempo de Atención de Avería, al tiempo transcurrido desde que se realiza la generación del ticket de avería reportada al PROVEEDOR hasta la subsanación y restitución del servicio el cual debe ser comunicado al MIDIS para la verificación respectiva.
g. Toda actividad o provisión de bienes que tenga que ejecutar el PROVEEDOR para subsanar la avería serán sin costo alguno para el MIDIS, salvo el caso en que la avería sea imputable a la Entidad. En dicho escenario, el PROVEEDOR deberá redactar un oficio al MIDIS detallando el motivo por el que le atribuye las causas de la avería al MIDIS.
h. El PROVEEDOR deberá brindar un número telefónico para que el MIDIS a través de la Oficina General de Tecnología de información (OGTI) reporte la avería.
i. El PROVEEDOR deberá informar a la Oficina General de Tecnología de información (OGTI) mediante correo electrónico grp_sa@midis.gob.pe, cuando la avería haya sido resuelta. Este requisito será indispensable para contabilizar el "tiempo de atención de avería".
j. El MIDIS podrá reportar averías de lunes a domingo bajo un servicio 24x7, incluyendo feriados.
k. Como parte del Informe mensual del servicio se deben incluir el detalle y causas de la avería, acciones correctivas realizadas y tiempo de solución empleado para restablecer el servicio.
l. El proveedor brindara equipo móvil con un plan de datos, para el monitoreo del servicio.
m. El PROVEEDOR deberá brindar el siguiente plazo de atención y soporte técnico:

N°	Descripción	Detalle	Tiempo Máximo de resolución (minutos)
1	Tiempo para generar el ticket de avería.	Tiempo empleado por el PROVEEDOR para generar el ticket de avería. El tiempo se contabiliza desde que el MIDIS reporta a la mesa de ayuda del PROVEEDOR mediante el número 0800 u otro.	Hasta 30 minutos.
2	Tiempo de resolución de avería para Perdida del servicio	Tiempo empleado por el PROVEEDOR para restablecer el servicio de conectividad de datos cuando el motivo de la avería sea por causa de hardware, software de los equipos de comunicación de propiedad del PROVEEDOR, por algún daño en el medio físico de transmisión o incidente de seguridad de la información	Hasta 4 horas tiempo que se contabiliza desde que se cuenta con el código de ticket. En caso se requiere el remplazo del equipo hasta 8 horas.
3	Tiempo de deterioro, intermitencia del servicio. No implica una interrupción permanente del servicio	Tiempo empleado por el PROVEEDOR para brindar el soporte correctivo, resolver la avería reportada y restablecer el servicio de acceso a internet para el MIDIS. El tiempo se contabiliza desde que el PROVEEDOR genera el ticket de avería al MIDIS.	Hasta 24 horas, tiempo que se contabiliza desde que se cuenta con el código de ticket.

4.8. OTRAS OBLIGACIONES POR PARTE DEL PROVEEDOR

a. El servicio de instalación se realizará en horario fuera de oficina (inclusive fin de semana), en coordinación con el personal de la Oficina de Tecnología de Información.
b. En ninguna circunstancia, deberá paralizar las actividades de los usuarios en las sedes, dentro de horario de oficina.
c. La Oficina General de Tecnologías de la Información, designará al personal responsable, quien realizará las coordinaciones y supervisión de los trabajos de instalación.
d. El proveedor deberá considerar todos los equipos, materiales y accesorios necesarios para la instalación y configuración de los equipos, enlaces y servicios suministrados.
e. El proveedor brindará una capacitación de todas las soluciones brindadas en el servicio por veinte (20) horas como mínimo de manera virtual sobre las soluciones de Seguridad Perimetral (6 horas), Administración de Ancho de Banda (6 horas), Mitigación DDoS (4 horas) y Protección de Aplicaciones Web (4 horas). Deberá entregar constancias de participación para tres (03) personas, Cabe indicar que la capacitación solicitada es de carácter no oficial y podrá ser dictado por personal propio del contratista o partner estratégico.

5. PLAZO DE EJECUCIÓN DEL SERVICIO

5.1. PLAZO DE IMPLEMENTACIÓN DEL SERVICIO

El plazo de implementación del servicio será de sesenta (60) días calendario como máximo, contabilizados a partir del día siguiente de la firma del contrato, este período comprende, la instalación y puesta en producción completa del servicio.

La aceptación de la implementación del servicio se realizará mediante un "**acta de implementación del servicio**", firmado por el proveedor y la Oficina General de Tecnología de información del MIDIS.

5.2. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio será de veinticuatro (24) meses contados desde el día siguiente de firmada el "**acta de inicio del servicio**", el acta de inicio del servicio deberá firmarse por el contratista y la Oficina General de Tecnología de información del MIDIS luego que se concluya con la implementación y se suscriba el acta de implementación.

6. LUGAR DE LA EJECUCIÓN DEL SERVICIO

El servicio será brindado en la Sede Central del Ministerio de Desarrollo e Inclusión Social ubicado en Av. Paseo de la República 3101 San Isidro, Lima, para lo cual el contratista deberá respetar las medidas de seguridad establecidas por el MIDIS.

7. ENTREGABLES

El contratista deberá presentar los siguientes entregables por mesa de partes del MIDIS. Toda la documentación que se detalla a continuación será validada y aprobada por la Oficina General de Tecnología de Información.

7.1. ENTREGABLE 1 – PLAN DE TRABAJO

Este documento debe ser entregado hasta los siete (07) días calendario, contabilizados al día siguiente de la firma del contrato en el que se detalla las actividades de implementación del servicio, el cual deberá incluir como mínimo lo siguiente:

a. Diagrama de la arquitectura propuesta y detallada (interconexión, redes, protocolos, etc.)
b. Plan y cronograma de implementación del servicio.

7.2. ENTREGABLE 2 – IMPLEMENTACIÓN DEL SERVICIO

El contratista deberá presentar un informe técnico adjuntando el "acta de implementación del servicio", hasta los cinco (05) días calendarios, tras haber implementado el servicio, el mismo que deberá incluir como mínimo lo siguiente:

a. Relación y documentación técnica de los componentes instalados para brindar el servicio
b. Diagrama de conectividad, diagramas físicos de conexión de equipos y su integración con la red del MIDIS.
c. Protocolo de atención ante incidencias que afecten la operatividad del servicio.
d. Protocolo de pruebas y funcionalidades aprobadas por la Oficina de Tecnología de la Información (OGTI).
e. Debe incluir los datos (nombre, correo electrónico, teléfono móvil, etc.) de cada contacto según el escalamiento correspondiente
f. Acta de capacitación sobre la solución implementada.

7.3. ENTREGABLES MENSUALES DEL SERVICIO

El Contratista deberá entregar mensualmente (al cierre de cada mes) un informe técnico detallado en el cual evidencie la calidad del servicio, hasta los diez (10) días calendarios el cual deberá incluir como mínimo lo siguiente:

a. Consumo de ancho de banda de cada enlace contratado (detalles de tráfico de subida y descarga).
b. Informe de averías (fecha, duración, motivos, acciones de remediación, recomendaciones).
c. Estado actual de los equipos de comunicación que forman parte de la solución (uso de recursos de CPU, memoria, interfaces, etc.)
d. Informe técnico sobre incidencias detectadas por los componentes de la seguridad perimetral, DDoS, administrador de ancho de banda, protección de aplicaciones Web, IaaS y SOC.

Con el primer entregable mensual del servicio, el contratista deberá incluir el "**acta de inicio del servicio**".

8. SEGUROS

El Proveedor debe presentar copia simple del SCTR (Seguro Complementario de Trabajo de Riesgo), del personal que realizará los trabajos de configuración y montaje de la solución propuesta. Este seguro debe ser presentado junto con la documentación solicitada en dentro del entregable 1- Plan de Trabajo, el cual debe indicar la cobertura y vigencia de la misma (debiendo mantenerse vigente hasta la culminación de la implementación del servicio).

9. REQUISITOS DEL POSTOR Y PERSONAL CLAVE

Los requerimientos mínimos que debe cumplir el postor y personal clave:

9.1. REQUISITOS DEL POSTOR

a. Tener Registro Único de Contribuyente habilitado.
b. Tener Código de Cuenta Interbancario registrado.
c. Tener Registro Nacional de Proveedores vigente

9.2. REQUISITOS DEL PERSONAL CLAVE

El proveedor de servicio debe incluir dentro de su personal tres (03) profesionales como mínimo:

- Un (01) Jefe de Proyecto (Clave):

  Funciones o actividades a desarrollar

  - Realizar el seguimiento y monitoreo durante la implementación del servicio. o Coordinar con personal de la Oficina General de Tecnologías de la Información, la correcta instalación y funcionamiento del servicio.
  - Supervisar la correcta instalación, configuración y capacitación del servicio.

  Formación académica
  - Ingeniero titulado de Sistemas y/o Ingeniería Informática y/o Ingeniería Electrónica y/o ingeniería Industrial y/o Ingeniería de Comunicaciones y/o Ingeniería de sistemas e informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Redes y Telecomunicaciones y/o Ingeniería de Software.

  Experiencia o Contar con experiencia mínima de tres (03) años en la gestión y/o planificación y/o coordinación y/o supervisión de la implementación de proyectos de internet y/o servicio de datos y/o seguridad de la información.

- Un (01) Especialista en Seguridad Perimetral tipo1:

  Funciones o actividades a desarrollar

  - Realizar la instalación y configuración de los equipos de seguridad Perimetral realizando las pruebas y la puesta en producción del mismo.
  - Coordinar con personal de la Oficina General de Tecnologías de la Información, la configuración de cada equipo de seguridad del servicio.

  Formación académica o Perfil: Técnico titulado o Bachiller de Ingeniería de Sistemas y/o Informática y/o Electrónica y/o Industrial y/o Redes y Comunicaciones y/o Sistemas e

Informática y/o Telecomunicaciones y/o Computación y Sistemas y/o Computación e Informática y/o Redes y Comunicaciones de datos.

Capacitación y Experiencia o Un Especialista debe contar con certificación oficial del fabricante de la solución de Seguridad Perimetral.

- Contar con experiencia mínima de dos (02) años en la Implementación y configuración de Proyectos de Internet y/o Seguridad de la Información

- Un (01) Especialista en Seguridad Perimetral tipo2:

Funciones o actividades a desarrollar

- Realizar la instalación y configuración de los equipos de seguridad Perimetral realizando las pruebas y la puesta en producción del mismo.
- Coordinar con personal de la Oficina General de Tecnologías de la Información, la configuración de cada equipo de seguridad del servicio.

Formación académica o Técnico titulado o Bachiller de Ingeniería de Sistemas y/o Informática y/o Electrónica y/o Industrial y/o Redes y Comunicaciones y/o Sistemas e Informática y/o Telecomunicaciones y/o Computación y Sistemas y/o Computación e Informática.

Capacitación y Experiencia o El Especialista debe contar con curso del fabricante o parnert autorizado o con la certificación oficial del fabricante de la solución de Mitigación DDoS.

- Experiencia: Contar con experiencia mínima de dos (02) años en la Implementación y configuración de Proyectos de Internet y/o Seguridad de la Información.

Las certificaciones del especialista tipo 1 y tipo2 deberán ser a nivel técnico no se aceptaran como válidas certificaciones a nivel de ventas y/o preventa.
Los documentos de los profesionales para el cargo de (01) Especialista en Seguridad Perimetral tipo1 y Un (01) Especialista en Seguridad Perimetral tipo2, serán presentados para la firma del contrato.

10. CONFORMIDAD DEL SERVICIO

La conformidad del servicio será otorgada en un plazo máximo de siete (07) días calendario por la Oficina General de Tecnologías de la Información, acompañado del informe técnico emitido por el especialista a cargo de la supervisión del servicio, previa presentación por parte del contratista de los entregables descritos en el numeral 7.

11. FORMA DE PAGO

Los pagos del servicio se realizarán en forma mensual por un periodo de veinticuatro (24) meses en armadas iguales, previa conformidad por parte de la Oficina General de Tecnologías de la Información, dentro de los diez (10) días calendario siguientes de otorgada la conformidad, siempre que se verifiquen para ello las condiciones establecidas en el contrato

12. CLAUSULA DE CONFIDENCIALIDAD

Toda información del MIDIS a que tenga acceso el Contratista, así como su personal, es estrictamente confidencial. El Contratista y su personal deben de comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito del MIDIS.

Sobre la inobservancia del párrafo anterior, esta se entenderá como un incumplimiento que no puede ser revertido, por lo que se procederá a la resolución del contrato, bastando para ello una comunicación notarial.

A fin de ejercer el cumplimiento, el Contratista deberá presentar una declaración jurada para la firma del contrato en la cual confirme que mantendrá las reservas del caso sobre toda la información que el MIDIS comparta.

13. PENALIDADES

13.1. PENALIDAD POR MORA EN LA EJECUCIÓN DEL SERVICIO

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

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

Donde:

F = 0.40 para plazos menores o iguales a sesenta (60) días.
Plazo = plazo vigente en días
Monto = Monto total del contrato

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 no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

13.2. OTRAS PENALIDADES

Se aplicará penalidad por cada hora de no atención y solución de incidencias y/o averías, luego de superado el plazo descrito a continuación:

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Cuando el proveedor demora más de 30 minutos en la generación del ticket de avería o fallas del servicio	0.2 % del monto mensual	Se procederá a emitir un informe indicando el tiempo de retraso el cual será aplicado en el primer mes de la ejecución del servicio
2	Cuando el proveedor demora más de 90 minutos en la solución de una avería (pérdida total del servicio)	5% del monto mensual	Evaluación en informe mensual de conformidad y descuento en la facturación mensual del servicio contratado
3	Cuando el proveedor demore más de 4 horas en la recuperación del servicio por causa de equipos o conexión física dañada. En caso del reemplazo de equipo demore más de (8) horas, contabilizados desde la entrega del ticket de atención.	8% del monto mensual	Evaluación en informe mensual de conformidad y descuento en la facturación mensual del servicio contratado

14. PLAZO MÁXIMO DE RESPONSABILIDAD DEL CONTRATISTA

De acuerdo al artículo 40 del Texto Único Ordenado de la Ley N° 30225 Ley de Contrataciones del Estado y el artículo 173 de su reglamento, el contratista es responsable por la calidad ofrecida y por los vicios ocultos del servicio por un plazo de un (1) año, contado a partir de la conformidad final de la prestación otorgada por la Entidad.

15. CLÁUSULA ANTICORRUPCIÓN

El Contratista declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el Contratista se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado. Además, El Contratista se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Importante
Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el comité de selección incorpora los requisitos de calificación previstos por el área usuaria en el requerimiento, no pudiendo incluirse requisitos adicionales, ni distintos a los siguientes:

3.2. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos: El proveedor deberá estar en el registro vigente de empresas prestadoras de servicios de valor añadido, expedida por Ministerio Transportes y Comunicaciones - MTC **Importante** *De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.* Acreditación: Copia del certificado de registro de empresa prestadora del servicio valor añadido, expedida por el Ministerio de Transportes y Comunicaciones. **Importante** *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	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: Jefe de Proyecto: Ingeniero titulado de Sistemas y/o Ingeniería Informática y/o Ingeniería Electrónica y/o ingeniería Industrial y/o Ingeniería de Comunicaciones y/o Ingeniería de sistemas e informática y/o Ingeniería

de Telecomunicaciones y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Redes y Telecomunicaciones y/o Ingeniería de Software.

Acreditación:

El título profesional o grado de bachiller requerido será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda.

Importante para la Entidad

El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso título profesional o grado de bachiller requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

B.4 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

Jefe de Proyecto:
Contar con experiencia mínima de tres (03) años en la gestión y/o planificación y/o coordinación y/o supervisión de la implementación de proyectos de internet y/o seguridad de la información.

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

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.

Importante

- *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 (25) años anteriores a la fecha de la presentación de ofertas.*
- *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 2, 000,000.00 (Dos millones con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: Servicios de Internet en general brindados mediante fibra óptica y/o servicio de Internet Dedicado y/o Enlace de Datos y/o servicio de Acceso Dedicado a Internet y/o servicio de internet a nivel nacional y/o servicio de acceso a internet. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[9], correspondientes a un máximo de veinte (20) contrataciones. 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 (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) 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. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso 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° 9.** Cuando en los contratos, órdenes de servicios 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 servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

[9] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"… 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. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"
(…)
"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*

- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV
FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

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

FACTOR DE EVALUACIÓN		PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A.	**PRECIO**	
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 máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **100 puntos**

Importante
Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de los Términos de Referencia ni los requisitos de calificación.

CAPÍTULO V
PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, 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 del **"Servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social"**, que celebra de una parte el **MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL - MIDIS**, en adelante **LA ENTIDAD**, con RUC Nº 20545565359, con domicilio legal en Av. Paseo de la República N° 3101 – San Isidro, representada por **JOSE ENRIQUE TAFUR VELIT**, identificado con DNI N° 09387184, designado mediante Resolución Ministerial N° 023-2023-MIDIS y facultado para suscribir contratos mediante Resolución Ministerial Nº D000001-2024-MIDIS, 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 comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° 004-2024-CS/MIDIS** para la contratación del **"Servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social"**, 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 objeto el **"Servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social"**.

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 servicio, 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 del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO[10]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en soles, en pagos periódicos, en forma mensual por un periodo de 24 meses en armadas iguales, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

- Informe del funcionario responsable de la Oficina General de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada, acompañado del informe técnico emitido

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

por el especialista a cargo de la supervisión del servicio.
- Comprobante de pago.
- Entregables correspondientes, según lo indicado en el numeral 7 de los términos de referencia.

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 de producida la recepción, 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 quince (15) días, bajo responsabilidad de dicho funcionario.

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

En caso de retraso en el pago por parte de LA ENTIDAD, 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 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de veinticuatro (24) meses contados desde el día siguiente de firmada el "acta de inicio del servicio", el acta de inicio del servicio deberá firmarse por el contratista y la Oficina General de Tecnología de Información del MIDIS luego que se concluya con la implementación y se suscriba el acta de implementación.

El plazo de implementación del servicio será de sesenta (60) días calendario como máximo, contabilizados a partir del día siguiente de la firma del contrato, este período comprende, la instalación y puesta en producción completa del servicio, en concordancia con lo establecido en el expediente de contratación.

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.

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, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

Importante
Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente: *"De fiel cumplimiento del contrato:* [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD 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 por el literal a) del numeral

155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la Oficina General de Tecnologías de la Información, acompañado del informe técnico emitido por el especialista a cargo de la supervisión del servicio, en el plazo máximo de siete (7) días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD 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.

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

CLÁUSULA DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (1) año contado a partir de la conformidad final de la prestación otorgada por LA ENTIDAD.

CLÁUSULA DUODÉCIMA: PENALIDADES

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

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

Donde:

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

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 no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante
De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

OTRAS PENALIDADES

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Cuando el proveedor demora más de 30 minutos en la generación del ticket de avería o fallas del servicio	0.2 % del monto mensual	Se procederá a emitir un informe indicando el tiempo de retraso el cual será aplicado en el primer mes de la ejecución del servicio
2	Cuando el proveedor demora más de 90 minutos en la solución de una avería (pérdida total del servicio)	5% del monto mensual	Evaluación en informe mensual de conformidad y descuento en la facturación mensual del servicio contratado
3	Cuando el proveedor demore más de 4 horas en la recuperación del servicio por causa de equipos o conexión física dañada. En caso del reemplazo de equipo demore más de (8) horas, contabilizados desde la entrega del ticket de atención.	8% del monto mensual	Evaluación en informe mensual de conformidad y descuento en la facturación mensual del servicio contratado

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

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA CUARTA: 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 QUINTA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS[11]

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación 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 de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El arbitraje será institucional y resuelto por árbitro único nombrado por el Centro que administre el arbitraje cuando la cuantía de la controversia sea igual o menor a las 10 UIT. Si la cuantía supera las 10 UIT o la controversia involucra alguna pretensión indeterminada las partes acuerdan que se resolverá por un tribunal arbitral conformado por tres (03) integrantes.

LA ENTIDAD y EL CONTRATISTA en virtud a lo señalado en el numeral 226.1 del artículo 226 del Reglamento de la Ley de Contrataciones del Estado, encomiendan la organización y administración del arbitraje al Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú o al Centro de Arbitraje de la Cámara de Comercio de Lima.

Las partes acuerdan que los plazos aplicables dentro de las reglas del arbitraje serán los siguientes:
- Plazo para demandar, contestar o reconvenir: 20 días hábiles. (El mismo plazo operará para interponer y absolver excepciones, objeciones y cuestiones probatorias).
- Plazo para reconsiderar resoluciones distintas al laudo y absolver la misma: 10 días hábiles.
- Plazo para solicitar y absolver la interpretación, exclusión, integración o rectificación del laudo: 15 días hábiles.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

La entidad no está obligada a constituir una fianza bancaria como requisito para suspender la obligación de cumplimiento del laudo y su ejecución arbitral o judicial; siendo este acuerdo oponible a cualquier reglamento del Centro de Arbitraje que administre el proceso arbitral.

CLÁUSULA DÉCIMA OCTAVA: 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.

---

[11] De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

CLÁUSULA DÉCIMA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: Av. Paseo de la República N° 3101 – San Isidro

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 (15) 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"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales[12].

[12] Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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[13]		Sí		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 reducción de la oferta económica.
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 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[14]

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

[13] Esta información será verificada por la Entidad 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 postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

[14] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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[15]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[16]		Sí		No	
Correo electrónico :					

Datos del consorciado ...					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[17]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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 reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.

[15] En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad 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 numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

[16] Ibídem.

[17] Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[18]

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del representante común del consorcio

Importante
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

[18] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO Nº 2

DECLARACIÓN JURADA
(ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
Presente.-

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

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iv. 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.

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

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

vii. 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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social, de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante
Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo de veinticuatro (24) meses contados desde el día siguiente de firmada el "acta de inicio del servicio", el acta de inicio del servicio deberá firmarse por el contratista y la Oficina General de Tecnología de Información del MIDIS luego que se concluya con la implementación y se suscriba el acta de implementación.

El plazo de implementación del servicio será de sesenta (60) días calendario como máximo, contabilizados a partir del día siguiente de la firma del contrato, este período comprende, la instalación y puesta en producción completa del servicio, en concordancia con lo establecido en el expediente de contratación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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 al **CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, 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 [.....].

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]	[%][19]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%][20]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[21]

[CONSIGNAR CIUDAD Y FECHA]

---

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

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

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

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1 o de su Representante Legal	**Nombres, apellidos y firma del Consorciado 2 o de su Representante Legal**
Tipo y N° de Documento de Identidad	**Tipo y N° de Documento de Identidad**

Importante
De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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
Servicio de internet dedicado para el Ministerio de Desarrollo e Inclusión Social	
TOTAL	

El precio de la oferta en soles 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 servicio a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán 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

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *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]".

ANEXO Nº 7

DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV

Lima , de de 20

Señores
OFICINA DE ABASTECIMIENTO
CONCURSO PÚBLICO N° 004-2024-CS/MIDIS
Presente. -

Asunto: **Autorización para el pago con abono en cuenta**.

Por la presente autorizo a usted, el abono a mi cuenta, según la siguiente información:

Código Interbancario:

A nombre de:

Nombre del Banco:

Tipo de Cuenta: Moneda S/.

RUC (**Asociado** al CCI)

En el caso de estar sujeto a detracción sírvase indicar la respectiva cuenta: Retención
Detracción
Banco de la Nación

Asimismo, dejo constancia que el comprobante de pago a ser emitido por mi representada una vez cumplida o atendida la correspondiente Orden de Compra y/o de Servicio quedará cancelado para todos sus efectos mediante la sola acreditación del importe del referido comprobante de pago a favor de la cuenta en la entidad bancaria a que se refiere el primer párrafo de la presente.

Tener en cuenta que, si el RUC no está asociado al CCI indicado, NO se podrá efectuar el pago respectivo.

Atentamente,

Firma:

Nombres y apellidos:
DNI:
Denominación/Razón Social:
RUC:

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [22]	FECHA DE LA CONFORMIDAD DE SER EL CASO[23]	EXPERIENCIA PROVENIENTE[24] DE:	MONEDA	IMPORTE[25]	TIPO DE CAMBIO VENTA[26]	MONTO FACTURADO ACUMULADO [27]
1										
2										
3										
4										

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

[23] Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) 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.

[24] Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN *"Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz"*. Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, *"... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá 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 podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe"*.

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

[26] 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 Servicios o de cancelación del comprobante de pago, según corresponda.

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [22]	FECHA DE LA CONFORMIDAD DE SER EL CASO[23]	EXPERIENCIA PROVENIENTE[24] DE:	MONEDA	IMPORTE[25]	TIPO DE CAMBIO VENTA[26]	MONTO FACTURADO ACUMULADO [27]
5										
6										
7										
8										
9										
10										
	...									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante

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 del Estado con Sanción Vigente en http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 10

AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 004-2024-CS/MIDIS
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] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o Representante legal o común, según corresponda

Importante
La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.

Difusión de la Política del Sistema Integrado de Gestión

Somos una entidad dedicada a mejorar la calidad de vida de la población en situación de pobreza, riesgo, vulnerabilidad y abandono del país, coordinando y articulando las intervenciones con los diferentes actores vinculados, promoviendo el ejercicio de derechos, acceso a oportunidades y el desarrollo de las propias capacidades, somos conscientes del impacto positivo en la ciudadanía, el fortalecimiento de la confianza y la credibilidad en nuestro Ministerio, por lo que nos comprometemos a:

1. *Dedicar nuestros esfuerzos a la provisión de un servicio eficaz, oportuno y pertinente a las necesidades de nuestros/as usuarios/as con el fin de lograr su satisfacción;*
2. *Incentivar la identificación e implementación de la mejora continua del SIG;*
3. *Salvaguardar la confidencialidad, integridad y disponibilidad de la información, identificando vulnerabilidades y amenazas y aplicando gestión de riesgos en los activos de la información;*
4. *Cumplir con los requisitos del SIG desde la Alta Dirección conjuntamente con las servidoras y los servidores del MIDIS, independientemente del régimen laboral o modalidad contractual en la que presten servicios.*

Finalmente, el MIDIS recuerda a la ciudadanía sus canales de atención de denuncias sobre presuntos actos de corrupción en el siguiente enlace: https://www.gob.pe/21129-denunciar-un-presunto-acto-de-corrupcion?child=17010, a fin de que denuncien cualquier hecho contrario a ley, garantizando la reserva de la identidad del denunciante.