

BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

Aprobado mediante Directiva N° 001-2019-OSCE/CD



Organismo
Supervisor de las
Contrataciones
del Estado

*SUB DIRECCIÓN DE NORMATIVIDAD - DIRECCIÓN TÉCNICO NORMATIVA
ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE*

SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div> <div>Importante</div> <ul style="list-style-type: none"> • Abc </div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div> <div>Advertencia</div> <ul style="list-style-type: none"> • Abc </div>	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div> <div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz </div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases estándar deben ser elaboradas en formato WORD, y deben tener las siguientes características:

Nº	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo

8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

1. Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.
2. La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.

*Elaboradas en enero de 2019
Modificadas en junio 2019, diciembre de 2019 y julio 2020*

f

Bp

φ

**BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA
CONTRATACIÓN DE SERVICIOS EN GENERAL**

CONCURSO PÚBLICO N° 007-2021-MML-GA-SLC

**SERVICIO DE ACCESO CORPORATIVO A INTERNET CON
SEGURIDAD GESTIONADA PARA LA MUNICIPALIDAD
METROPOLITANA DE LIMA**

Handwritten mark resembling a stylized 'A' or 'P'.

Handwritten mark resembling a stylized 'P'.

Handwritten signature or mark.



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)

1
P
G

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.

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 manifestamente 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). 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 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 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.

Handwritten signature or mark.

Handwritten signature or mark.

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.

1

2

3

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.

Importante

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 original, 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.

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 accesorio, 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 cien mil Soles (S/ 100,000.00), 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.

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-emitar-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 : MUNICIPALIDAD METROPOLITANA DE LIMA
RUC N° : 20131380951
Domicilio legal : JR. CONDE DE SUPERUNDA 141 - CERCADO DE LIMA
Teléfono: : 01-6321300
Correo electrónico: : fernando.santamaria@munlima.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado Formato de Aprobación de Expediente de Contratación S/N, el 19 de mayo de 2021.

1.4. FUENTE DE FINANCIAMIENTO

RECURSOS DIRETAMENTE RECAUDADOS

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 **TREINTA Y SEIS (36) MESES** contados a partir de la suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio, en concordancia con lo establecido en el expediente de contratación.

El plazo de implementación máximo será de **setenta y cuatro (74) DÍAS CALENDARIO** contados a partir del día siguiente de la suscripción del contrato.

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 S/. 5.00 (Cinco con 00/100 soles) en Caja de la Entidad, sito en el Pasaje Santa Rosa N°172 - 180, Cercado de Lima.

1.10. BASE LEGAL

- TUO de la Ley N° 30225, Ley de Contrataciones del Estado, en adelante la Ley
- Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento, modificado mediante Decreto Supremo N° 377-2019-EF
- Directivas del OSCE.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Decreto Supremo N° 008-2008-TR, Reglamento de la Ley MYPE.
- Decreto Supremo N° 013-2013-PRODUCE - Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial.
- Ley N° 31084 - Ley de Presupuesto del Sector Público para el Año Fiscal 2021.
- Ley N° 31085 - Ley de Equilibrio Financiero del Presupuesto del Sector Público del Año Fiscal 2021.
- Código Civil

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.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos¹, 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.

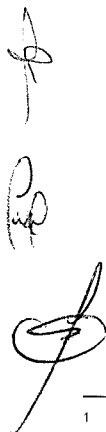
En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

El certificado de vigencia de poder expedido por registros públicos no debe tener una antigüedad mayor de treinta (30) días calendario a la presentación de ofertas, computada desde la fecha de emisión.

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.
- 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) Declaración jurada de plazo de prestación del servicio. (**Anexo N° 4**)
- f) 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 N° 5**)
- g) El precio de la oferta en Soles debe registrarse directamente en el formulario electrónico del SEACE. Adicionalmente se debe adjuntar el Anexo N° 6 cuando el postor goza de alguna exoneración legal.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales.

¹ La omisión del índice no determina la no admisión de la oferta.



Importante

- *El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.*

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.

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. Carta Fianza y/o Póliza de Caucción.
- 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.
- 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.
- f) Domicilio y correo electrónico para efectos de la notificación durante la ejecución del contrato.
- g) Detalle de los precios unitarios del precio ofertado².
- h) Estructura de costos³.
- i) Nombre completo de la persona de contacto, números de teléfonos y correos electrónicos para las coordinaciones durante la ejecución contractual.
- j) Pólizas de seguros SCTR del personal clave.
- k) Nombres y documentos de identificación del personal clave propuesto.
- l) Certificado de antecedentes penales y policiales del personal clave propuesto.
- m) Certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS a fin de asegurar el cumplimiento de las especificaciones de IPv6 y que puedan funcionar de manera segura sin inconvenientes.
- n) El contratista deberá presentar una carta del fabricante indicando que la solución implementada para brindar el servicio Anti-DDoS se encuentra con vigencia tecnológica a fin de que la protección de la red de la Entidad este actualizada en cuando las últimas modalidades y tipos de ataques.

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 original, 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. Para dicho efecto*

² Incluir solo en caso de la contratación bajo el sistema a suma alzada.

³ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

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 REMYPE, 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.

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 Haya⁴.

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 en la Subgerencia de Logística Corporativa de la Municipalidad Metropolitana de Lima, sito en Jr. Conde de Superunda N° 141 - 3er piso – Cercado de Lima, de lunes a viernes en el horario de 08:30 a 13:00 y de 14:00 a 16:00 horas.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos mensuales, de la siguiente manera:

El pago por el concepto del servicio se contabiliza a partir del día siguiente de suscrita el Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio. El monto mensual se determinará del 100% del monto adjudicado, el cual se mantendrá fijo y no estarán sujetos a reajuste alguno, durante el periodo de treinta y seis (36) meses.

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

- Informe del servicio mensual por parte del área técnica de la Subgerencia de Gobierno Digital e Innovación emitiendo la conformidad de la prestación efectuada. Previo Informe mensual del Servicio contratado emitido por el contratista.
- Comprobante de pago.

Dicha documentación debe ser dirigida a la Subgerencia de Gobierno Digital e Innovación y se debe presentar en Mesa de Partes de la Municipalidad Metropolitana de Lima.

⁴ Según lo previsto en la Opinión N° 009-2016/DTN.

**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

**LOS TERMINOS DE REFERENCIA SE ENCUENTRAN EN
ANEXO ADJUNTO EN LA PARTE FINAL DE LAS BASES**



3.2. REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El contratista debe acreditar un monto facturado acumulado equivalente a S/ 3,500 000.00 (Tres Millones Quinientos Mil 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.</p> <p>Se consideran servicios similares a los siguientes:</p> <ul style="list-style-type: none">• Servicio de Transmisión de Datos mediante fibra óptica• Transmisión de datos a través de red privada virtual• Transmisión digital o de comunicaciones digitales• Servicio de seguridad de red,• Servicio de seguridad perimetral• Servicio de Internet• Servicios de transmisión de dato. <p><u>Acreditación:</u></p> <p>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 pago⁵, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>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 N° 7 referido a la Experiencia del Postor en la Especialidad.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>

⁵ 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 fehacencia 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".

	<p>la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 8.</p> <p>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.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 7 referido a la Experiencia del Postor en la Especialidad.</p>
	<p>Importante</p> <ul style="list-style-type: none"> 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".
B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Un (01) Jefe de Proyecto: Con título en Ingeniería en Electrónica, Ingeniería Industrial, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Computación y Sistemas.</p> <p>Un (01) Supervisor Con Bachiller o título en Ingeniería Electrónica, Ingeniería Industrial, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Computación y Sistemas</p> <p>Seis (6) Técnicos para la implementación del servicio. Profesional técnico en redes y comunicaciones o Sistemas o informática o electrónica y/o Bachiller o titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería electrónica o Ingeniería Industrial o Ingeniería de Telecomunicaciones</p> <p><u>Acreditación:</u></p> <p>El Título profesional o Grado de bachiller 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: http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En Título profesional o Grado de bachiller 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.</p> <p>Importante para la Entidad</p> <p><i>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.</i></p>
B.3.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>Un (01) Jefe de Proyecto:</p>

	<p>Certificado o Diplomado como Profesional en Project Management. El contratista deberá documentar lo solicitado.</p> <p>UN (01) Supervisor</p> <p>Certificado en la marca propuesta como asociado o profesional o experto en routing y/o switching y/o firewalling, el mismo que deberá estar vigente o activo (comprobable en base a una referencia on-line o certificada del fabricante), se deberá indicar dicha referencia y el código del certificado para su verificación. El contratista deberá documentar lo solicitado.</p> <p>Dos (02) Técnico Perfil 1</p> <p>Certificación de especialista o profesional en routing y switching de la marca propuesta.</p> <p>Dos (02) Técnico Perfil 2</p> <p>Certificación de especialista o profesional en firewalling de la marca propuesta.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias, y/o certificados y/o diploma.</p> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p>
B.4	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p><u>Un (01) jefe de Proyecto</u></p> <p>Con cuatro (04) años como Jefe de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.</p> <p><u>Un (01) supervisor</u></p> <p>El supervisor deberá contar con experiencia mínima de cuatro (04) años como jefe o supervisor de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.</p> <p><u>Seis (06) Personal Técnico</u></p> <p>Dos (02) técnicos con dos (02) años de experiencia como mínimo en actividades de routing y switching</p> <p>Dos (02) técnicos con dos (02) años de experiencia en actividades con firewalling</p> <p>Dos (02) técnicos con dos (02) años de experiencia en Administradores de Ancho de Banda</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>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.</p> <p>Importante</p> <ul style="list-style-type: none">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.

- | | |
|--|---|
| | <ul style="list-style-type: none">• 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. |
|--|---|

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.
- 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		
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante registro en el SEACE o el documento que contiene el precio de la oferta (Anexo N° 6), según corresponda.		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: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta P _i = Puntaje de la oferta a evaluar O _i = Precio i O _m = Precio de la oferta más baja PMP = Puntaje máximo del precio 100 puntos
PUNTAJE TOTAL		100 puntos

CAPÍTULO V
PROFORMA DEL CONTRATO

Conste por el presente documento, el contrato del **Servicio de Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima**, que celebra de una parte la MUNICIPALIDAD METROPOLITANA DE LIMA, en adelante LA ENTIDAD, con RUC N° 20131380951, con domicilio legal en el JR. CONDE DE SUPERUNDA N° 141 - CERCADO DE LIMA, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], 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° 007-2021-MML-GA-SLC** para la contratación del **Servicio de Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima**, 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 la contratación del **SERVICIO DE ACCESO CORPORATIVO A INTERNET CON SEGURIDAD GESTIONADA PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA**.

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 PAGO⁶

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles en pagos mensuales, 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.

El pago por el concepto del servicio se contabiliza a partir del día siguiente de suscrita el Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio. El monto mensual se determinará del 100% del monto adjudicado, el cual se mantendrá fijo y no estarán sujetos a reajuste alguno, durante el periodo de treinta y seis (36) meses

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, 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

⁶ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 **TREINTA Y SEIS (36) MESES** contados a partir de la suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio, en concordancia con lo establecido en el expediente de contratación.

El plazo para la implementación máximo **será de setenta y cuatro (74) DÍAS CALENDARIO** contados a partir del día siguiente de la suscripción del contrato.

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 Carta Fianza 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 **Subgerencia de Gobierno de Digital e Innovación** en el plazo máximo de siete (7) días de producida la recepción de la documentación siguiente:

La conformidad de la implementación del servicio será otorgada luego de recibido la siguiente documentación por parte del contratista:

- Informe de instalación y funcionamiento del servicio, adjuntando documentos indicados en el acápite entregables.

La conformidad de la prestación mensual del servicio luego de recibido lo siguiente por parte del contratista:

- Informe mensual del Servicio contratado
- Comprobante de pago.

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 cumpliera 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 TRES (3) años contados a partir de la conformidad 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;

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.

OTRAS PENALIDADES

En la fase de ejecución del servicio:

1. Cuadro de Penalidades para el servicio de Acceso a Internet

Interrupciones del servicio imputables al contratista (corte parcial, total de los componentes del servicio descritos en el Cuadro de Penalidades)	Porcentaje de disponibilidad de los componentes del servicio de acceso corporativo a Internet:	% Deducible de la facturación mensual
	• Medios de transmisión del proveedor.	
	• Equipos de comunicaciones del proveedor.	
	Mayor o igual a 99.90%	0%
	Menor a 99.90% y Mayor o igual a 99.75%	5%
	Menor a 99.75% y Mayor o igual a 99.50%	6%
	Menor a 99.50 % y Mayor o igual a 99.00%	7%
	Menor a 99.00% y Mayor o igual a 98.00%	8%
	Menor a 98.00% y Mayor o igual a 97.00%	9%
	Menor a 97.00%	20%

En caso de aplicarse la penalidad en tres (03) meses consecutivos o seis (06) no consecutivos la entidad podrá resolver el contrato por incumplimiento.

100% = 24 horas x n (n = días del mes. Por ejemplo: en marzo, n=31; en abril, n=30)

Para efectos del cálculo de la penalidad, se acumularán las horas en las que el servicio se haya interrumpido en el mes. Para este cálculo se tomará en cuenta que el 100% equivale al número total de horas mensuales.

En los casos en que se produzca un retraso en la atención de averías, y el motivo del retraso sea imputable a las gestiones de acceso al local u otras causas atribuibles a la MML, se considerará una "parada de reloj" la cual será registrada por personal de la MML y se reanudará una vez superado el inconveniente a efectos de llevar el control de los tiempos de atención requeridos en los términos de referencia del servicio.

2. Por el incumplimiento de soporte técnico de los SLA la penalidad será la siguiente:

Ítem	Demora de tiempo en solución	Valor de la Penalidad
1	De 1 a 3 horas	20% de una UIT
2	De 4 a 5 horas	60% de una UIT
3	De 6 a 8 horas	80% de una UIT
4	Mayor a 9 horas	70% de una UIT por cada hora de incumplimiento

Otros casos sujetos a penalización se consideran en el siguiente cuadro:

N°	SUPUESTO DE APLICACIÓN DE PENALIDADES	FORMULA DE CALCULO
1	Cuando el contratista realice la rotación y/o reemplazo del personal clave, sin comunicar a la Subgerencia de Gobierno Digital e Innovación.	5 % de UIT por cada ocurrencia
2	Cuando el Contratista incumpla con el cambio de equipo ya sea por falla de fabricación o desperfecto del equipo o porque no aplique configuraciones de seguridad o funcionalidad que sean necesarias para el servicio.	10% de la UIT por cada día pasado el tiempo de solución.
3	Cuando el contratista no cumpla con el traslado del servicio secundario y el traslado y configuración de los equipos de seguridad gestionada a otra sede que requiera el área usuaria.	10 % de la UIT por cada día de retraso
4	Cuando el contratista no cumpla con el plazo establecido para la implementación del servicio	10 % de la UIT por cada día de retraso

PROCEDIMIENTO

La SGDI, al advertir el incumplimiento, levantará un informe el cual será comunicado a la Subgerencia de Logística Corporativa para la aplicación de penalidad respectiva.

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

Handwritten signatures and a circular stamp with the number 27.

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.

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 CONTROVERSIAS⁷

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 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.

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.

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:

⁷ 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).

DOMICILIO DE LA ENTIDAD: JR. Conde de Superunda N° 141 – Cercado de Lima.

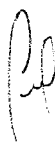
DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

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"



ANEXOS



ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [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 ⁸	Sí	No	
Correo electrónico :			

Autorización de notificación por correo electrónico:

... [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios⁹

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.

⁸ 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 original, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el artículo 149 del Reglamento.

⁹ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los cien mil Soles (S/ 100 000.00), 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 N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 ¹⁰		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹¹		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹²		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

¹⁰ 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 original, en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 149 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹¹ Ibidem.

¹² Ibidem.

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios¹³

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.

¹³ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los cien mil Soles (S/ 100 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.
- iv. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables del TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- v. 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 N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- vi. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vii. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- viii. 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 N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima**, 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 N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 **TREINTA Y SEIS (36) MESES** contados a partir de la suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio, en concordancia con lo establecido en el expediente de contratación.

El plazo de implementación máximo **será de setenta y cuatro (74) DÍAS CALENDARIO** contados a partir del día siguiente de la suscripción del contrato.

[CONSIGNAR CIUDAD Y FECHA]

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



ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 N° 007-2021-MML-GA.SLC**.

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] [%]¹⁴

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁵

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%¹⁶

[CONSIGNAR CIUDAD Y FECHA]

¹⁴ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁵ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

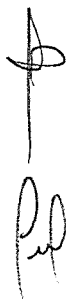
¹⁶ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

.....
Consortiado 2
Nombres, apellidos y firma del Consortiado 2
o de su Representante Legal
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 N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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 Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima	
TOTAL	

El precio de la oferta 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 N° 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA-SLC
Presente.-.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ¹⁷	FECHA DE LA CONFORMIDAD DE SER EL CASO ¹⁸	EXPERIENCIA PROVENIENTE ¹⁹ DE:	MONEDA	IMPORTE ²⁰	TIPO DE CAMBIO VENTA ²¹	MONTO FACTURADO ACUMULADO ²²
1										
2										
3										
4										

¹⁷ 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.

¹⁸ 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 período.

¹⁹ 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".

²⁰ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²¹ 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.

²² Consignar en la moneda establecida en las bases.

MUNICIPALIDAD METROPOLITANA DE LIMA
CONCURSO PUBLICO N° 007-2021-MML-GA-SLC

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ¹⁷	FECHA DE LA CONFORMIDAD DE SER EL CASO ¹⁸	EXPERIENCIA PROVENIENTE ¹⁹ DE:	MONEDA	IMPORTE ²⁰	TIPO DE CAMBIO VENTA ²¹	MONTO FACTURADO ACUMULADO ²²
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 N° 8

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2021-MML-GA.SLC
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] absorbida 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]

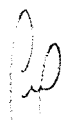
.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

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
DE LOS TERMINOS DE REFERENCIA**





Municipalidad Metropolitana de Lima
Subgerencia de Gobierno Digital e Innovación

TÉRMINOS DE REFERENCIA

SERVICIO DE ACCESO CORPORATIVO A INTERNET CON SEGURIDAD GESTIONADA PARA LA MUNICIPALIDAD METROPOLITANA DE LIMA



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:07:14 -05:00



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:13:49 -05:00



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 14:53:53 -05:00

SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN
GERENCIA DE ADMINISTRACIÓN



MUNICIPALIDAD METROPOLITANA DE LIMA
SURGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

REQUERIMIENTO

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima

2. FINALIDAD PÚBLICA

La Municipalidad Metropolitana de Lima, para el logro de sus objetivos estratégicos de brindar servicios de calidad a los ciudadanos de Lima, lleva a cabo procesos y actividades estratégicas, tácticas y operativas que requieren de servicios básicos indispensables para su realización y cumplimiento, tales como son, los servicios de conectividad a Internet basados en altos estándares tecnológicos y de seguridad.

El servicio será para los colaboradores de la MML para la ejecución de los diferentes procesos internos de las dependencias que por su naturaleza utilizan el servicio para la comunicación con diferentes instituciones públicas y privadas. Asimismo, el servicio requerido permitirá brindar en forma continua, oportuna y eficiente, servicios públicos municipales con soporte a diferentes canales y medios de comunicación, incrementando la calidad del acceso a los servicios que brinda la entidad, en beneficio de los ciudadanos de Lima Metropolitana.

3. ANTECEDENTES

La Municipalidad Metropolitana de Lima, cuenta actualmente con el servicio de Acceso Corporativo a Internet y Seguridad Gestionada con un ancho de banda de servicio principal de 400 Mbps y un servicio de contingencia de 200 Mbps. Por lo que para el logro de sus objetivos estratégicos requiere contar con un mejor servicio de calidad para usuarios de la MML y los ciudadanos de Lima. Para ello lleva a cabo procesos y actividades estratégicas, tácticas y operativas que requieren de servicios básicos indispensables para su realización y cumplimiento, tales como son, los servicios de conectividad a Internet basados en altos estándares tecnológicos y de seguridad gestionada.

De lo indicado, la MML es una organización con 20 Sedes y aproximadamente 6000 usuarios conectados a través de una Red LAN y dispositivos móviles con salida hacia la WAN mediante una cabecera centralizada.

4. OBJETIVOS DE LA CONTRATACIÓN

Objetivo General:

Contratar el Servicio de Acceso Corporativo a Internet y Seguridad Gestionada de acuerdo a las características técnicas descritas en el presente documento, que permita a las unidades orgánicas de la MML el normal desarrollo de sus actividades institucionales.

Objetivo Específico:

- Contar con un Servicio de Acceso Corporativo a Internet con Seguridad Gestionada para la MML para garantizar los servicios de conectividad a Internet con características de alta disponibilidad y capacidad.
- Asegurar la Seguridad Gestionada y soporte técnico del servicio

Firma digital



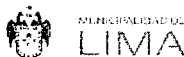
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 14:54:30 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:14:17 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:07:38 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Proveer de Seguridad Perimetral, mecanismos de detección y respuesta que permitan proveer continuidad de los servicios de Internet de manera segura y administrada.

5. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

5.1. DESCRIPCIÓN DEL SERVICIO A CONTRATAR

El Servicio de Acceso Corporativo a Internet con Seguridad Gestionada para la Municipalidad Metropolitana de Lima, comprende lo siguiente:

ITEM	SERVICIO	CANTIDAD	UNIDAD
1	SERVICIO DE INTERNET	1	SERVICIO

Se requiere implementar el servicio de acceso a Internet con seguridad gestionada (Equipamiento dedicado para la defensa de la red perimetral, así como la protección contra ataques de DDoS basada en la nube del contratista, una solución WAF On-Premise, Administrador de Ancho de Banda y End-Point protection and Response (EDR) o Detección y Respuesta de Amenazas para servidores). Todo el equipamiento propuesto deberá ser nuevo, de primer uso y no deberán de tener anuncio de end of life ni en of sales.

Para asegurar la operatividad, gestión y calidad, el contratista debe garantizar la interconexión del equipamiento asignado a los servicios solicitados, motivo por el cual el servicio se considera integral e indivisible y consta de dos (02) componentes (Principal y Contingencia):

ÍTEM	SERVICIO	DIRECCIÓN	TIPO DE ENLACE	ANCHO DE BANDA	
				PRINCIPAL	CONTINGENCIA
1	Servicio de internet	Calle Conde de Superunda N° 141 Cercado de Lima	Simétrico	800 Mbps	300 Mbps

Los requerimientos mínimos que deberá cumplir el CONTRATISTA para implementar los servicios de Internet de contingencia y seguridad gestionada son los siguientes:

5.1.1 Servicio de acceso a Internet para la sede central de la MML

Se deberá brindar un servicio de acceso a Internet mediante fibra óptica para la Sede Principal de la MML, ubicada en Jr. Conde de Superunda 141-Cercado de Lima, Lima.

- Un (01) enlace de acceso a Internet, de tipo simétrico, dedicado, de 800 Mbps de ancho de banda como enlace primario activo, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio físico fibra óptica en los tramos local e internacional. El contratista debe garantizar que el ancho de banda proporcionado sea el mismo desde la puerta de enlace hasta la salida internacional.
- Un (01) enlace de acceso a Internet, de tipo simétrico, dedicado de 300 Mbps de ancho de banda, como enlace secundario pasivo, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio de acceso fibra óptica, además la ruta y el nodo empleado tiene que ser diferente a la ruta del enlace principal.
- El contratista deberá ser parte del NAP (Network Access Point) Perú y garantizar un enlace dedicado con conexión directa y overbooking 1:1 al NAP Perú.
- El contratista deberá contar con un sistema de servidores DNS redundantes donde se deberá registrar las direcciones IP públicas de la MML.



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- La solución deberá estar preparada para soportar hasta un 30% más de la velocidad requerida (800 Mbps en Principal, 300Mbps en Secundario), sin necesidad de cambiar el equipamiento ni generar costos para la Entidad.
- El contratista proporcionará como mínimo 64 direcciones IPs versión 4, públicas válidas para la publicación de los servicios de la institución (incluidas ip broadcast, ip de red y gateway) repartidas en ambos routers para los servicios de internet, las mismas serán de uso exclusivo de la MML.
- En caso la entidad tenga el requerimiento de direcciones ip publicas versión 6, el contratista deberá proveer hasta un 30% del total de ips publicas versión 4 solicitadas, sin costo para la MML
- El contratista debe considerar que el enlace secundario y los equipos de redundancia que forman parte del servicio, deben estar disponibles para ser trasladado a otra sede de la MML (Jiron Rufino Torrico cuadra 12, Plaza Francia - Cercado de Lima), en caso requiera la necesidad del área usuaria, sin que esto genere costo adicional a la MML. La dirección descrita corresponde al primer traslado, el segundo (posible) traslado, será determinado durante la ejecución del servicio y en el Cercado de Lima.
- Los equipos de redundancia que forman parte del servicio que sean trasladados a otra sede que disponga el área usuaria, serán configurados y/o reconfigurados sin que esto genere costo adicional a la MML. La cantidad de traslado será hasta en dos ocasiones durante la vigencia del contrato. Las sedes donde se instalen los equipos de redundancia contarán con un enlace de fibra oscura.

5.1.2 Sub-Componente A: Administrador de Ancho de Banda (Un equipo):

Controlador de Optimización WAN el cual permita auditar, controlar y optimizar el tráfico de aplicaciones en los enlaces de la institución; se requiere que esté en capacidad de identificar en forma granular un mínimo de 2000 firmas de tráfico de capa 7, clasificándolas en grupos de forma automática según su naturaleza y mediante empleo de técnicas DPI, heurística (análisis de comportamiento) en adición a análisis en capa 7 (firmas). La solución debe ser totalmente integrada y debe estar en capacidad de cumplir con los siguientes requerimientos:

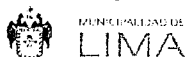
1. La solución propuesta debe estar en capacidad de entregar en cada dispositivo requerido los servicios de Visibilidad y Control en la misma unidad proporcionando todas las licencias de Software para tal fin y sin hardware o dispositivos externos adicionales provenientes de la misma o de diferente marca.
2. El sistema debe almacenar al menos 1 año de estadísticas detalladas en disco duro dentro del mismo dispositivo independiente de la presencia de un sistema de colección externa.
3. El equipamiento deberá ser un hardware appliance de propósito específico.
4. Deberá contar con 4 puertos de interfaz 10/100/1000/10000 Mbps (cobre como mínimo).
5. Deberá tener dos (02) fuentes de poder que operen en alta disponibilidad.
6. La solución no paraliza el tráfico de red hacia el internet; por lo tanto, en el caso probable de presentarse algún fallo en el equipo éste deberá activar una función de bypass.
7. La solución deberá poder identificar y detectar tipos de tráfico independiente de la aplicación que se esté utilizando tales como: P2P, Web, Mail, Multimedia, mensajería instantánea, videoconferencia, sesión remota, servicios para compartir archivos, mecanismos alternos de vpn (por explorador).
8. La solución deberá poder tener la capacidad de identificar y clasificar el tráfico en tiempo real y por histórico basados en la información de la aplicación (capa 7).

Firma digital



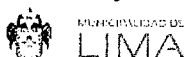
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V-B
Fecha: 17.05.2021 14:55:45 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V-B
Fecha: 15.05.2021 18:28:13 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V-B
Fecha: 15.05.2021 15:08:06 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

9. Control de ancho de banda por aplicaciones

10. La solución deberá contar con la capacidad de asignar determinados anchos de banda o políticas a las aplicaciones que se encuentren en las clases o grupos de estaciones.
11. La solución deberá contar con la capacidad de crear políticas de prioridades para la asignación de ancho de banda.
12. La solución de administración de ancho de banda deberá contar con una consola de administración local como una solución dentro del equipamiento o una solución adicional.
13. La solución de administración de Ancho de Banda deberá contar con características de aceleración de tráfico.
14. La solución deberá contar con la capacidad de priorizar tráficos de categorías web o protocolos TCP o UDP, direcciones IP, grupos de direcciones IP y/o contenido.
15. La solución debe soportar IPv4 e IPv6
16. La solución debe soportar SNMP v2 y/o v3
17. La solución debe contar con la capacidad de asignación de ancho de banda por rango horario.
18. La solución deberá contar con un throughput de 4 Gbps, pero licenciado a 800 Mbps.
19. Cantidad de host IP soportados a través del equipamiento: 400000.
20. La solución deberá contar con la totalidad de licencias para atender las características técnicas mínimas solicitadas.
21. El proceso de descubrimiento y análisis estadístico del tráfico debe ejecutarse en background y en forma continua, mientras la solución se encuentra en operación, sin la intervención de un administrador y debiendo ser continuo en el tiempo, la solución deberá ser amigable e intuitiva.
22. El equipo deberá contar con un almacenamiento para reportes, por lo menos con 1 año de antigüedad.
23. Los reportes deberán proporcionar las capacidades de poder exportarse en PDF o csv, mostrando la capacidad consumida de ancho de banda utilizado por los hosts; asimismo deberá mostrar el consumo en tiempo real de ancho de banda por dirección IP o categoría.
24. La solución de administración de ancho de banda deberá contar con la capacidad de soporte para el protocolo IPv4 e IPv6 totalmente activada.
25. Debe tener acceso mediante HTTP, HTTPS, SSH, Telnet y consola mediante puerto serial, que permita la gestión de políticas y administración del equipo.
26. Debe tener la capacidad de enviar los logs hacia un servidor syslog.
27. La solución debe soportar al menos 20.000 conexiones por segundo

□ 5.1.3 Sub-Componente B: Firewalls de Seguridad Perimetral en Alta Redundancia (dos appliance)

El servicio de protección de redes estará basada en dos (02) equipos con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.

Aspectos Generales:

- El servicio consiste en una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- La solución ofrecida debe ser en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas.
- El fabricante debe aparecer en el cuadrante relacionado a los líderes en el ranking



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

del último informe de Forrester Wave Enterprise Firewalls

- El fabricante debe aparecer en el cuadrante relacionado a los líderes en el ranking del último informe de Forrester Wave Automated Malware Analysis.
- El fabricante deberá tener una efectividad de seguridad mayor o igual al 95% según el último reporte de NSS Labs para Next Generation Firewall.
- La plataforma propuesta por el fabricante debe contar con la certificación para trabajar IPv6 tanto en Firewall como en IPS o debe estar certificado en USGv6 para trabajar en IPv6
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el contratista.
- Como parte de la propuesta, el contratista deberá proporcionar acceso a una herramienta virtual (software) que nos permita evaluar buenas prácticas, configuraciones por realizar antes de impactar en el escenario de producción, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución.
- Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere que la propuesta incluya documentación pública sobre dicha herramienta explicando su alcance.
- La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.
- El contratista, dentro del periodo de contrato, debe ofrecer una herramienta de análisis de ciberseguridad que permita detectar comportamiento anómalo que estén ocurriendo dentro de la red y de esta manera permita identificar el origen de este comportamiento y poder ejecutar acciones preventivas antes que impacte en los servicios críticos. Además, que permita tomar correcciones necesarias de protección compartiendo información con las soluciones de seguridad.
- Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, el contratista deberá tener la facilidad de contactar de forma directa con el Fabricante, el cual incluye:
 - Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas.
 - Análisis de logs e indicadores de compromiso
 - Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas.
 - Recomendaciones de pasos siguientes a realizar.

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V- B
Fecha: 17.05.2021 14:57:52 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V- B
Fecha: 15.05.2021 18:15:24 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V- B
Fecha: 15.05.2021 15:08:35 -05:00

Capacidad

- Throughput de Next Generation Firewall de 5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

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.

- Throughput de Prevención de Amenazas de 2.8 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), 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.
- No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
- El equipo debe soportar como mínimo 1 millón de sesiones simultáneas y 55 mil nuevas sesiones por segundo, medidos en capa 7 (con paquetes HTTP de 1 byte) o su equivalente de 13 millones de sesiones simultáneas y 300 mil nuevas sesiones por segundo, medidos en capa 4 (con paquetes TCP).
- Debe contar con fuente de poder redundante con capacidad de cambio en caliente.
- Disco de estado sólido interno de 240 GB o superior.
- Mínimo 12 interfaces de red 10/100/1000/ formato RJ45 para tráfico de datos de la red
 - Mínimo 4 interfaces de red 1G en formato SFP para el tráfico de datos de la red
 - Mínimo 4 interfaces de red 10G en formato SFP+ para el tráfico de datos de la red

Características Generales

- El dispositivo de seguridad 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, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- 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.
- Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- Permitir NAT de destino basado en dominio en lugar de IP. Opcionalmente, el equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
- Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- Soportar túneles GRE como punto inicio o finalización del túnel.
- 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.
- Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN
de contextos o dominios virtuales.

Alta Disponibilidad

- Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
- 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.
- 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.
- Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

Funcionalidades de Firewall

- 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.
- Deberá incluir la capacidad de creación de políticas basadas en la integración con servidores a los servicios de autenticación vía Active Directory, LDAP.
- 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.
- Permitir el agendamiento de las políticas de seguridad.
- Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
- Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría.
- 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).
- Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- Debe poseer mecanismos para la integración con directorio activo mediante el protocolo LDAP

Descifrado de tráfico SSL/TLS

- Debe permitir descifrar el tráfico de navegación de usuarios (LDP/AD) a internet mediante la instalación de un certificado digital en los equipos.
- 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.
- Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- Debe ser capaz de inspeccionar el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
- Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 14:59:15 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Luz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 16:16:00 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:09:10 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

descifrado al tráfico SSL/TLS

- Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
- Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
- Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.
- Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (opcionalmente, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

Control de Aplicaciones

- 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.
- Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- 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.
- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos u otros criterios.
- 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.
- 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, identificando el consumo de en Bytes, Hits y visualizar las fechas de las políticas, Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

Prevención de Amenazas

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.

- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
- Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.
- 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.
- Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
- Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
- Los eventos deben identificar el país que origino la amenaza.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- 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; todos tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

Análisis de malware de día cero

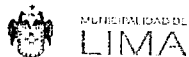
- La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero, utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.
- En caso de tratarse de una plataforma de Sandboxing Cloud, deberá cumplir con los siguientes requerimientos:
 - El Next Generation Firewall debe tener capacidad de analizar 100 archivos por minuto al Sandbox Cloud.
 - Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines)
 - Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
 - Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
 - El Next Generation Firewall 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.
 - 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, FedRAMP.
 - Deberá contar con una acreditación que el servicio se encuentra alineado a los estándares HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) y PCI (Payment Card Industry Data Security Standard). Esta acreditación deberá ser dada por una entidad tercera al fabricante.
- En caso de tratarse de una plataforma de Sandboxing On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá ser capaz de analizar alto números de elementos, sin sufrir degradación ni encolamiento y haciendo uso completo de técnicas de emulación y análisis dinámico, así mismo también pueden considerar

Firma digital



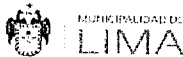
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:00:47 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:16:27 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:10:05 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Firmas, Prefiltros, Machine Learning

- o Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo), con el objetivo de mantener los controles de ciberseguridad en caso de falla de uno de los equipos.
- o Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows, MacOS, Linux y Android.
- o Debe admitir topologías de implementación en modo sniffer o en línea (in-line)
- 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.
- Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.
- 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.
- 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 (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.
- Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- 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 ó 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.
- Permitir la subida de archivos al sandbox de forma manual y vía API.
- Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- 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 y/o la solución debe deshabilitar totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

Filtro de contenido WEB

- Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- 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.
- Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.
- Debe permitir la creación de categorías personalizadas.
- Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
- Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
- Debe permitir la customización de la página de bloqueo.
- Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
- Debe permitir notificar al usuario, mostrándole sólo una página de alerta, pero



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

permitiéndole continuar la navegación al site.

- 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.
- Debe contar con una lista permanentemente actualizada que permita identificar y bloquear los sitios web más peligrosos (top de malware, top de phishing, etc) provenientes de la web del fabricante o algún sitio de confianza.

Protección avanzada de DNS

- 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.
 - 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.
 - La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA o equivalentes)
 - Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos (DGA o equivalentes)
 - Debe poseer políticas para bloquear dominios (DGA o equivalentes) o interrumpir las consultas de DNS a dichos dominios.
 - Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS
 - 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.

Identificación de usuarios

- 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.
- 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.
- Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI ó sistema de monitoreo log de la marca ofertada.
- Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, y/o Soluciones NAC y/o Proxy, vía Syslog y/o XFF (X-forward-for) en la cabecera HTTP y/o XML API y/o protocolo propietarios de la marca propuesta para la identificación de direcciones IP y usuarios.
- Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- Debe permitir la definición de grupos dinámicos de usuarios (opcional).

QOS

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.
- Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.
- El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
- Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
- Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.

Filtro de datos

- Los archivos deben ser identificados por extensión y firmas.

Firma digital



MUNICIPALIDAD DE
LIMA
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:02:16 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA
Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Luz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:17:01 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA
Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:11:07 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.

VPN

- No deberá requerir licenciamiento alguno y deberá soportar como mínimo 2000 conexiones recurrentes.
- Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
- La VPN IPSec debe soportar como mínimo:
 - DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
 - Autenticación MD5, SHA-1, SHA-2;
 - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
 - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- 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.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
 - Antes del usuario se autentique en la estación;
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
 - Bajo demanda del usuario;
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, MacOS X.
- Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- Debe permitir el bloqueo de uso de VPN que no sean las permitidas por esta administración

Consola de administración y monitoreo

- 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 realizarse dentro de los mismos appliances de seguridad o appliance físico/virtual dedicado independiente del mismo fabricante.
- Permitir exportar las reglas de seguridad en formato CSV y PDF
- 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.
- Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- 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



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- destino)
- Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- 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.
- Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- Debe permitir exportar e importar diferentes versiones de archivos de respaldo de configuración (backup)
- Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- 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;
- Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoria de configuraciones, eventos de sistema.
- Debe poder visualizar datos históricos de log, eventos, incidencias, análisis de tráfico por un tiempo mínimo de un año de antigüedad.
- 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.

□ 5.1.4 Sub-Componente C: Licencias de EDR (80 licencias)

- Se requiere el licenciamiento para ochenta (80) Endpoint para servidores entre virtuales y físicos: Windows 7, Windows 8, Windows 10, Windows Server: 2008R2, 2012, 2012R2, 2016, Linux, Sun Solaris, backups, con vigencia de mantenimiento por tres (03) años, según el cuadro de Servidores de la MML.

Servidores	Cantidad
Virtuales	58
Físicos	9
Total 67	

La cantidad solicitada es de 80 licencias para los 67 servidores (Virtuales: 58, físicos: 9) y un crecimiento del 20% que corresponde a 13 licencias proyectas a un futuro.

- Todos los componentes que forman parte de la solución deben ser suministrados por un solo fabricante y en idioma español o inglés.
- La Solución Endpoint, debe contemplar las siguientes características mínimas:
 - Las Licencias deben soportar los sistemas operativos: Windows 7, Windows 8, Windows 10, Windows Server: 2008R2, 2012, 2012R2, 2016, Linux, Sun Solaris (opcional).



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- o Serán distribuidas a los dispositivos finales a instalarse, los mismos que deberá de sincronizar con la consola cloud que será proporcionada por el CONTRATISTA y proporcionará la visibilidad de las reglas de monitoreo eliminación y cuarentena; según los archivos maliciosos que detecte.

Prevención contra exploits

- Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows, MacOS, Linux y Sun Solaris
- Mitigación de vulnerabilidades conocidas, desconocidas y día cero.
- Soporta técnicas de explotación de vulnerabilidades distintas, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc.
- Protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box".
- Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación, incluyendo aquellas desarrolladas internamente.
- Capacidad de crear un snapshot de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.
- Es posible configurar perfiles de protección en modo de prevención o monitoreo.
- Terminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación.
- Debe defenderse contra ataques avanzados persistentes/de día cero, que incluyen, pero no se limitan a:
 - o Malware general.
 - o Ataques de día cero.
 - o Explotar la vulnerabilidad de software existente.
 - o Ransomware.
 - o Spyware.
 - o Amenazas persistentes avanzadas/Ataques dirigidos
 - o Rootkits.
 - o Amenazas polimórficas.
 - o Amenazas combinadas.
 - o Malware ofuscado, malware desconocido y ataques de día cero.
 - o Scripts maliciosos que aprovechan: PowerShell, Visual Basic, Perl, Python, Java/JAR.
 - o Ataques residentes en la memoria y otros ataques sin malware.
 - o Ataques basados en documentos (archivos PDF y macros).
 - o Ataques de inicio de sesión remoto y el uso malicioso de software legítimo.
 - o Malware conocido y variantes que incluyen ransomware basado en malware.
- Capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.
- Identificación y prevención de intentos de escalamiento de privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac, Linux y Sun Solaris (opcional).
- Debe ser de propósito específico y no una solución derivada de Antivirus y que haya sido evaluada por MITRE ATT&CK.

Prevención contra malware.

- Utiliza un modelo matemático o técnica de aprendizaje generado a partir de aprendizaje de máquina para comparar cientos de características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows y Mac.
- Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.

0

[Firma manuscrita]

[Firma manuscrita]

0

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:04:19 -05:00

[Firma manuscrita]

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:17:37 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:12:02 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- Prevención de ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.
- Capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.
- Capacidad de identificación y bloqueo de malware basado en reglas de comportamiento de amenazas. Estas reglas deberán estar de forma predeterminada y se deberán actualizar periódicamente por el fabricante.
- Capacidad de poder colocar los malware en una carpeta de cuarentena
- Capacidad de realizar escaneos a demanda y programados
- Capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola.
- Capacidad de proporcionar protección contra malware sin necesidad de una BD de firmas o heurística y sin necesidad de una herramienta de sandboxing.
- Será posible de configurar las políticas en modo de prevención o monitoreo.
- Capacidad de mostrar en una cadena gráfica de eventos la causa raíz que originó el evento malicioso.
- Creación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.
- Capacidad de conectarse permanente a la lista actualizada de los nuevos antivirus proporcionada por la web del fabricante o fuente de confianza para poder bloquearlos.

Escaneo de archivos ejecutables.

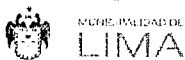
Permite realizar el escaneo de archivos ejecutables sin la necesidad de firmas.

- Permite programar el escaneo de archivos de manera semanal o mensual.
- El consumo de recursos al momento de realizar el escaneo debe de ser muy poco y no debe de impactar en la experiencia del usuario.
- Detectar componentes maliciosos en los archivos o cabeceras malformadas en la posible ejecución de estos.

Control de dispositivos

- Capacidad de controlar el uso de dispositivos con conexión vía USB para bloquear o permitir en acceso total o solo lectura.
- Los permisos podrán ser configurados con diferentes niveles de granularidad como: Marca, Producto, Serial Number
- Se podrán otorgar excepciones temporales para los permisos de dispositivos

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:04:55 -05:00

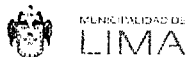
Protección contra el robo de contraseñas.

- Proporciona una protección predeterminada en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz, keylogger o similares.

Administración y revisión de eventos.

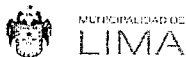
- Administración de políticas centralizada, vía una consola web.
- La consola distingue los eventos de prevención y notificación, y para cada uno de estos dos grupos clasifica los eventos en intentos de ejecución de exploits, intentos de ejecución de malware, violaciones a las políticas de restricciones e intentos de violación a las políticas de restricción.
- La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits.
- Permite la actualización y desinstalación del agente a partir de la consola.
- Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
- Cuenta con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizaciones de Active Directory
- Cada evento de prevención o notificación cuenta con información básica como

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:17:55 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:12:21 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

tipo de evento, módulo de la solución que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención, horario y fecha del evento, información forense (en caso de estar disponible).

- Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas.
- Permite la generación de reportes bajo demanda o programados y podrán ser enviados de forma automática a uno o más correos electrónicos.
- Capacidad de personalización del dashboard o widgets.
- Capacidad de tomar control remoto de los equipos Windows donde se encuentre instalado el agente, como mínimo deberá ser capaz de: 1) listar procesos, 2) listar carpetas y archivos, 3) ejecutar instrucciones por línea de comandos y Opcional: 4) ejecutar instrucciones basados en scripts de Python
- El formato de los reportes generados es PDF.
- La consola mantiene un historial de los reportes que han sido generados para su posterior consulta por el tiempo contratado.
- Soportar mediante upgrade de licencia funcionalidades de Endpoint Detection and Response (EDR) avanzado sin necesidad de instalar software adicional.
- Deberá de poder utilizar los datos capturados por el agente que se utiliza para realizar las tareas de detección e investigación, sin necesidad de utilizar un segundo agente.
- Deberá de contar con un dashboard que permite visualizar alertas generadas de distintas fuentes.
- Permite la visualización de eventos de manera histórica durante un periodo de tiempo determinado
- Deberá de poder mostrar el número total de alertas, incluyendo la cantidad de alertas que resultan de aplicar un filtro, y poder almacenar dicho filtro (opcional).
- El producto deberá implementar un menú contextual que permita analizar de manera detallada la alerta, generar una línea de tiempo, editar una regla, eliminar una alerta, copiar el URL de una alerta y copiar la alerta.
- El producto deberá demostrar el nombre de la computadora, su dirección IP, el nombre del proceso que generó la alerta y el número de la alerta en la parte superior para que el analista pueda consultarla con facilidad.

Análisis de alertas e investigación de actividad sospechosa

- El producto deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque.
- El producto deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso.
- El producto deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso (opcional), veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución.
- El producto deberá demostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos.
- El producto debería de poder identificar, de todas las actividades mencionadas anteriormente, aquellas que sean maliciosas o altamente sospechosas y separarlas en una categoría de fácil acceso para el analista.

Investigación de amenazas

- El producto deberá de tener la capacidad de realizar consultas a los datos capturados y almacenados.
- El producto deberá de poder realizar consultas diferenciando por ejecuciones



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- de un proceso o inyecciones de un proceso.
- El producto deberá de tener la capacidad de realizar consultas por actividad de los archivos considerando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
- El producto deberá de tener la capacidad de realizar consultas por la actividad de red entrante, saliente y fallida; por la actividad en el registro, particularmente la creación de llaves, la eliminación de llaves, cuando las llaves sean renombradas, cuando se configure un valor en las llaves o se elimine el valor de las llaves.
- Todas las búsquedas mencionadas anteriormente deberán de poder programarse para ser ejecutadas en un día y hora determinados por una ocasión, o de manera recurrente ya sea de forma diaria en un horario determinado o algún día de la semana en particular, en un horario en específico.
- Todas las búsquedas deberán de poder ser ejecutadas observando los resultados en tiempo real o permitiendo trabajar al analista mientras la búsqueda se ejecuta en segundo plano.

Configuración y elementos de identificación

- El producto deberá de contar con mecanismos de generación de alertas considerando el comportamiento mostrado por los procesos de las computadoras.
- Las alertas generadas por el comportamiento de los procesos no deberán de utilizar firmas o heurísticas.
- Cada alerta generada por el comportamiento de los procesos deberá de tener una descripción del comportamiento identificado.
- El producto deberá de permitir al analista definir comportamientos de procesos para que generen alertas.
- El producto deberá de permitir la generación de excepciones a los comportamientos de los procesos que hayan sido identificados como maliciosos o sospechosos.
- El producto deberá de soportar el uso de indicadores de compromiso tradicionales, incluyendo rutas de archivos, nombres de archivos, dominios, direcciones IP y hashes.
- Las alertas pueden ser enviadas por algún medio de forma automática (mensajería instantánea o mensaje de texto o correo electrónico o algún mecanismo parecido que cumpla la funcionalidad indicada).

Acciones de respuesta

- El producto deberá de permitir aislar de la red una computadora a partir de la detección de una actividad maliciosa.
- Deberá permitir una sesión de Live Terminal para ejecutar acciones en el equipo víctima tales como: Listar archivos, Listar procesos, Ejecutar una instrucción vía CMD, Opcional: Ejecutar instrucciones vía Python.

5.1.5 Sub-Componente D: Solución en la nube para la protección contra ataques de Denegación de Servicios (uno - 01)

Se solicita una solución basada en la nube del contratista y deberá presentar el tipo y marca de la solución además gestionará todas las políticas de configuración de protección con personal técnico encargado del MML, así como también durante el servicio deberá presentar informes mensuales de manera obligatoria sobre lo relacionado.

La red del operador deberá tener implementada una solución de protección DDoS implementada en su red y que deberá contar con las siguientes características mínimas:

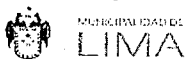
- El contratista deberá brindar un servicio de tráfico limpio en su nube local (territorio nacional), con disponibilidad al 99.90%, mediante el uso de una herramienta de mitigación de ataques de denegación de servicio dedicada. La solución deberá brindar protección para un volumen total de tráfico para el servicio de internet contratado.

Firma digital



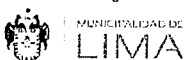
Firmado digitalmente por PAHNA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V. B
Fecha: 17.05.2021 15:06:14 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Luz FAU 20131380951 soft
Motivo: Doy V. B
Fecha: 15.05.2021 16:18:38 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V. B
Fecha: 15.05.2021 15:13:09 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- La solución propuesta deberá analizar tanto el tráfico de subida como tráfico de bajada y todos los servicios públicos que la entidad tenga o no dominio, e incluir la capacidad de detección de ataques de denegación de servicio a nivel de aplicación sin estados (stateless).
- La solución provista deberá ser de tipo appliance instalado en el site del contratista, de tecnología específica para la mitigación de ataques de denegación de servicios. No se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos Firewall, Next Generation Firewalls, Application Delivery Controllers, Routers u otros equipos de seguridad o redes.
- La solución de Mitigación DDoS deberá tener un sistema de creación automática de firmas en tiempo real para la protección frente a ataques emergentes de día cero.
- La solución de Mitigación DDoS deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos) que permita complementar el nivel de seguridad.
- La solución propuesta deberá ser de tipo Stateless.
- La solución propuesta deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on", también denominada en línea o siempre activa. No se aceptarán soluciones de mitigación de ataques de denegación de servicios bajo una arquitectura de derivación de tráfico.
- El contratista deberá brindar un reporte mensual de la actividad de seguridad relacionada a los ataques de denegación de servicios detectados y mitigados.
- Se requiere protección AntiDDoS SSL en la nube, con la capacidad de hacerlo de forma stateless, utilizando los certificados digitales que provea la entidad, con la capacidad de realizar autenticación de los usuarios en la sesión de SSL cuando se encuentra bajo ataque y finalmente, sin descifrar el tráfico limpio en tiempo de paz, para garantizar la confidencialidad.
- El contratista del servicio brindará reportes mensuales dentro de los 10 días del siguiente mes sobre el servicio de protección DDoS.

□ Sub-Componente E: Equipamiento Web Application Firewall – WAF (Dos appliance)

El Equipamiento proporcionado para dicha solución; deberá cumplir como mínimo con las siguientes características:

- Debe cumplir con las siguientes características de performance:
 - La solución debe soportar un Throughput en L4 de al menos 20 Gbps
 - La solución debe soportar un Throughput en L7 de al menos 20 Gbps
 - La solución debe soportar al menos 28 Millones de conexiones simultáneas
 - La solución debe soportar al menos 250.000 conexiones por segundo en L4
 - La solución debe soportar al menos 1 Millón HTTP Requests por Segundo

Funciones de seguridad

- Debe soportar seguridad SSL con las siguientes características:
 - Incluir mínimo 10,000 Transacciones por segundo SSL (RSA 2K Keys)
 - Incluir mínimo 6,500 Transacciones por segundo SSL (ECDSA P-256)
 - Soportar al menos 10 Gbps SSL Bulk Encryption (Throughput SSL)
 - Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits
- El Stack TLS de la solución debe soportar las siguientes funcionalidades/ características:
 - Session ID
 - Session Ticket
 - OCSP Stapling (online certificate status protocol)
 - Dynamic Record Sizing

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 solt
Motivo: Day V° B°
Fecha: 17.05.2021 15:07:14 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 solt
Motivo: Day V° B°
Fecha: 15.05.2021 18:19:01 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 solt
Motivo: Day V° B°
Fecha: 15.05.2021 15:13:30 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- o ALPN (Application Layer Protocol Negotiation)
- o Forward Secrecy

- La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)
- Debe soportar algoritmos de cifrado Camellia
- Firmado criptográfico de cookies para verificar su integridad.
- Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto), Opciona:Luna
- La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el

Servidor final, sin embargo, el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el tráfico SSL sin que el balanceador termine la sesión SSL.

- Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.
- Debe soportar HSTS (HTTP Strict Transport Security)
- Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.
 - o Scanners
 - o Exploits Windows
 - o Denial of Service
 - o Proxies de Phishing
 - o Botnets
 - o Proxies anónimos

- Funciones de WAF
- El WAF debe poder realizar la comprobación de estado a nivel de la aplicación de los servidores backend
- El WAF debe poder balancear la carga en los servidores back-end con mínimo los siguientes algoritmos de balanceo: round robin, menor conexión, respuesta más rápida.
- El WAF debe poder admitir el almacenamiento en caché y la compresión hasta de 5 Gb en una sola plataforma
- La solución WAF debe permitir el paso del tráfico cuando fallan los servicios
- El WAF debe poder realizar la optimización TCP / IP
- El WAF debe poder realizar el filtrado de paquetes o captura de paquetes.
- El WAF debe admitir el mirroring de SSL para habilitar la conmutación por error de SSL sin problemas
- El WAF debe ser compatible con TLS1.0, TLS1.1, TLS1.2 y TLS1.3
- El WAF debe admitir la aceleración de la criptografía de curva elíptica (ECC) en hardware
- El WAF debe admitir una curva elíptica de módulo primario de 384 bits
- El WAF debe soportar Camellia Ciphers Suites
- El WAF debe ser compatible con HTTP Strict Transport Security Support (HSTS) recomendado por las prácticas recomendadas de implementación de SSL Labs.
- El WAF debe admitir la función SSL de proxy que permite que el cliente se autentique directamente con el servidor y el servidor para autenticar al cliente según el certificado del cliente presentado
- El WAF debe admitir la funcionalidad de forward proxy SSL para crear dinámicamente un certificado SSL de servidor único antes de iniciar la conexión

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:07:53 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLÓRZANO Flor De
Luz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:19:19 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:25:17 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN
del lado del servidor.

- El WAF debe soportar autenticación de certificado de cliente
- El WAF debe poder proporcionar una función de bóveda segura para cifrar la clave privada SSL que se almacena en el dispositivo
- El WAF debe ser extensible con una licencia complementaria para proporcionar la autenticación de API y admitir OAuth 2.0.
- El WAF debe poder construir automáticamente políticas basadas en el tráfico detectado
- El WAF debe poder definir diferentes políticas para diferentes aplicaciones
- El WAF debe poder crear firmas o eventos de ataque personalizados
- El WAF debe poder crear y personalizar políticas de denegación de servicio
- El WAF debe tener un mecanismo de reversión de políticas
- El WAF debe ser capaz de hacer versiones de políticas
- El WAF debe tener un generador de políticas incorporado en tiempo real con autoaprendizaje automático y creación de políticas de seguridad
- El WAF debe tener plantillas de seguridad listas para la aplicación. P.ej. Microsoft Sharepoint, OWA, ActiveSync (opcional), SAP (opcional), Oracle Applications / Portal, PeopleSoft (opcional), Lotus Domino para una implementación rápida
- El WAF debe ser capaz de reconocer hosts de confianza
- El WAF debe poder aprender sobre la aplicación sin intervención humana.
- El WAF debe poder inspeccionar la política (auditoría + informes)
- El WAF debe poder proteger nuevas páginas de contenido y objetos sin modificaciones de políticas (opcional).
- 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). Puede aplicarse como parte de la aplicación de políticas para la prevención de anomalías.
- El WAF debe proporcionar seguimiento de sesión con capacidades mejoradas de generación de informes y cumplimiento que toman en cuenta las sesiones de usuario HTTP y los nombres de usuario de la aplicación dentro de la aplicación. Esto le brinda al administrador más información sobre actividades sospechosas de la aplicación (por ejemplo, quién fue el usuario detrás de un ataque) y más flexibilidad para aplicar la política de seguridad (como impedir que un determinado usuario use la aplicación). Se puede configurar si el sistema realiza un seguimiento de las sesiones según el nombre de usuario, la dirección IP o el número de identificación de la sesión.
- El WAF debe poder reemplazar / personalizar errores y páginas bloqueadas
- El WAF debe tener niveles de seguridad configurables.
- El WAF debe proporcionar una lista de las tareas de configuración pendientes de todo el sistema (por ejemplo, si hay una actualización de firmas disponible) y una lista de cuántas tareas de configuración de políticas de seguridad pendientes quedan para cada política de seguridad.
- El WAF debe entregar una puntuación de riesgo de la violación recibida
- El WAF debe poder integrarse con herramientas de pruebas de vulnerabilidad: Whitehat centinela (opcional), IBM Appscan, HP Webinspect y QualysGuard, para una rápida aplicación de parches virtuales.
- El WAF debe tener la capacidad de identificar y notificar fallas del sistema y pérdida de rendimiento (SNMP, syslog, correo electrónico, etc.)
- El WAF debe tener la capacidad de personalizar los registros (opcional).
- El WAF debe proporcionar un registro de solicitudes que admita los perfiles permitiendo que las entradas del registro de configuración se informen cuando se reciban solicitudes, que admita el registro de auditoría de solicitudes / respuestas HTTP / descifrados HTTPS, y permita que se emita la especificación de una respuesta cuando se produce una solicitud / respuesta

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:19:39 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:19:34 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:25:37 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACION

específica.

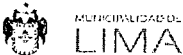
- El WAF debe proporcionar el registro de respuestas para ayudar a analizar los eventos de seguridad relacionados con la respuesta, por ejemplo. La protección de datos o las firmas de respuesta también son útiles para analizar infracciones de solicitudes, para determinar si representan un ataque real o un falso positivo (cuando WAF está configurado en modo transparente).
- El WAF debe tener capacidad para generar estadísticas de servicio y sistema. El panel de control muestra estadísticas de anomalías (el número de ataques de tipo de anomalía, solicitudes descartadas y total de violaciones de tipo de anomalía detectadas), un resumen del tráfico WAF (rendimiento, TPS y solicitudes por segundo) y los tipos de ataque detectados por el sistema. Puede filtrar todas las estadísticas según la aplicación web o la hora (última hora, día y semana).
- El WAF debe poder realizar la sincronización de la hora (ntp, etc.)
- El WAF debe proporcionar una vista de alto nivel de la actividad reciente en una sola pantalla, donde puede ver eventos agregados (incidentes) en lugar de transacciones individuales (que se muestran en la pantalla Solicitudes, los incidentes son presuntos ataques en la aplicación web)
- El WAF debe ser capaz de registrar eventos de seguridad con syslog
- El WAF debe ser capaz de registrar eventos de seguridad con SNMP
- El WAF debe poder monitorearse con SNMP para obtener información estadística
- El WAF debe poder monitorearse utilizando la versión 3 de SNMP
- El WAF debe proporcionar un registro integrado a sistemas de seguimiento de eventos de seguridad de terceros, como SIEM como Arcsight o Splunk
- El WAF debe admitir una API REST abierta que permita a los sistemas de terceros administrar completamente el WAF. Esto incluye la importación de la política de seguridad, detección de anomalías y perfiles de logging
- El WAF debe proporcionar el siguiente soporte HTTP / HTML:
- El WAF debe ser compatible con las versiones HTTP 1.0 y 1.1 o versiones superiores cuando estén disponibles en el mercado.
- El WAF debe ser compatible con la codificación de aplicación / x-www-form-urlencoded
- El WAF debe admitir v0 cookies o versiones superiores a medida que estén disponibles en el mercado.
- El WAF debe admitir las cookies v1 o versiones superiores a medida que estén disponibles en el mercado.
- El WAF debe hacer cumplir los tipos de cookies utilizados
- El WAF debe admitir la codificación fragmentada en las solicitudes o protección contra fragmentación
- El WAF debe admitir la codificación fragmentada en las respuestas o protección contra fragmentación
- El WAF debe soportar la compresión de solicitud
- El WAF debe soportar compresión de respuesta
- El WAF debe admitir la administración de flujos de aplicaciones y definir manualmente el flujo del sitio y las políticas de objetos
- El WAF debe soportar todos los juegos de caracteres durante la validación
- El WAF debe restringir los métodos utilizados, por ejemplo, GET, POST, todos los demás métodos
- El WAF debe restringir los protocolos y las versiones de protocolo utilizadas.
- El WAF debe admitir la codificación de idiomas de múltiples bytes.
- El WAF debe validar los caracteres codificados en URL
- El WAF debe restringir la longitud del método de solicitud
- El WAF debe restringir la longitud de la línea de solicitud
- El WAF debe restringir la longitud de URI de solicitud
- El WAF debe restringir la longitud de la cadena de consulta

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:20:36 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOIZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:19:49 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:24:52 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- El WAF debe restringir la longitud del protocolo (nombre y versión)
- El WAF debe restringir el número de encabezados
- El WAF debe restringir la longitud del nombre del encabezado
- El WAF debe restringir la longitud del valor del encabezado
- El WAF debe restringir la longitud del cuerpo de la solicitud
- El WAF debe restringir la longitud del nombre de la cookie
- El WAF debe restringir la longitud del valor de la cookie
- El WAF debe restringir el número de cookies.
- El WAF debe restringir la longitud del nombre del parámetro
- El WAF debe restringir la longitud del valor del parámetro
- El WAF debe restringir el número de parámetros
- El WAF debe restringir la longitud del parámetro combinado (nombres y valores juntos)
- 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 (% uXXYY)
 - Decodifique las entidades HTML (por ejemplo, c, & quot ;, & # xAA;)
 - Caracteres escapados (por ejemplo, \ t, \ 001, \ xAA, \ uAABB)
 - Técnicas de modelo de seguridad negativa
- El WAF debe protegerse contra:
 - Entrada no validada
 - Defectos de inyección
 - inyección SQL
 - Inyección OS
 - Manipulación de parámetros
 - Envenenamiento con cookies
 - Manipulación de campos ocultos
 - Fallas de secuencias de comandos de sitio
 - Desbordamientos de búfer
 - Control de acceso roto o controlar el acceso de los clientes a sus aplicaciones web y limitar la tasa de solicitudes
 - Autenticación rota y gestión de sesión
 - Manejo inadecuado de errores
 - Bombas XML / DOS
 - Navegación forzada o Brute force protection
 - Fuga de información sensible.
 - Secuestro de sesión
 - Negación de servicio
 - Solicitud de contrabando (opcional)
 - Manipulación de cookies
- El WAF debe poder configurar una lista de tipos de archivos permitidos para una aplicación web
- El WAF debe poder permitir o rechazar un tipo de archivo específico
- El WAF debe poder configurar una lista de URL permitidas para una aplicación web
- El WAF debe poder configurar una lista de parámetros permitidos para una aplicación web

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:21:47 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLÓRZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:20:13 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:24:30 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACION

- El WAF debe poder configurar una lista de cookies permitidas para su aplicación web
- El WAF debe poder configurar una lista de Métodos HTTP Permitidos para su aplicación web
- El WAF debe ser capaz de bloquear una lista específica de métodos HTTP
- El WAF debe poder configurar una lista de dominios de redirección permitidos para su aplicación web
- El WAF debe imponer la longitud máxima de los siguientes parámetros de solicitud HTTP:
 - Longitud de URL
 - Cadena de consulta (parámetros de URL)
 - Solicitud de longitud
 - Tamaño de datos POST
- El WAF debe poder imponer encabezados y valores HTTP específicos para que estén presentes en las solicitudes de los clientes
- El WAF debe ser compatible con la Aplicación de Solicitud de Dominio Cruzado HTML5 para permitir que un sitio web acceda a los recursos de otro sitio web utilizando JavaScript.
- El WAF debe poder imponer encabezados y valores HTTP específicos para que estén presentes en las solicitudes de los clientes
- El WAF debe ser capaz de definir los parámetros de las propias firmas de detección de ataques y ser alertado cuando se pasan umbrales para estos
- El WAF debe descargar y aplicar nuevas firmas automáticamente para garantizar una protección actualizada
- El WAF debe poder ocultar datos de huellas dactilares del sistema operativo de servidor de aplicaciones de fondo e información específica de la aplicación
- El WAF debe poder protegerse contra la actividad maliciosa dentro del código del lado del cliente incorporado (javascript, vbscript, etc ...)
- El WAF debe ser compatible con el encabezado de seguridad HTTP: Opciones de X-Frame, Opciones de X-Contenido-Tipo, Política de seguridad de contenido, Fijación de clave pública HTTP, Protección X-XSS, Bandera HttpOnly para cookies, Bandera segura para cookies
- El WAF debe ser compatible con la detección de ID de dispositivo y la huella digital
- El WAF debe ser compatible con el filtrado de tráfico WebSocket
- El WAF debe admitir la protección de credenciales sin agente cifrando en la capa de aplicación, encriptando las credenciales en tiempo real al momento de su envío. (Esto no considera el canal de comunicación encriptado, sino en tiempo real en el navegador)
- El WAF debe realizar el encubrimiento, por ejemplo, ocultando páginas de error y páginas de error de la aplicación e incluso datos específicos
- El WAF debe poder realizar la comprobación de virus en las cargas de archivos HTTP y los archivos adjuntos SOAP. Soporte a antivirus a través del canal de comunicación ICAP.
- El WAF debe poder brindar protección a las aplicaciones habilitadas para AJAX, incluidas aquellas que utilizan JSON para la transferencia de datos entre el cliente y el servidor. Esto incluye el soporte para configurar el comportamiento de respuesta de bloqueo de AJAX para aplicaciones que usan AJAX, de modo que si ocurre una infracción en una solicitud de AJAX, el sistema muestra un mensaje o redirige al usuario de la aplicación a otra ubicación.
- El WAF debe admitir la protección de los servicios web XML
- El WAF debe restringir el acceso a los servicios web XML a los métodos definidos a través del lenguaje de descripción de servicios web (WSDL) o el formato de esquema XML (XSD)

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Rubén Emilio FAU
20131380951 soft
Motivo: Day V° B°
Fecha: 17.05.2021 15:22:39 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V° B°
Fecha: 15.05.2021 18:20:32 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V° B°
Fecha: 15.05.2021 15:22:43 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- El WAF debe poder realizar la validación de los documentos XML de servicios web que cumplen con WS-I
- El WAF tiene una protección de analizador XML, limita las recursiones para frustrar las condiciones de DoS, limita el número de elementos, la longitud de los elementos, la aplicación de firmas de ataque. Además, se puede usar para cifrar y firmar documentos de acuerdo con el estándar WS-Security.
- El WAF debe poder realizar el enmascaramiento / barrido de la pantalla de información en las solicitudes y respuestas
- El WAF debe poder monitorear la latencia del tráfico de Capa 7 (capa de aplicación) para detectar los picos y anomalías en el patrón de tráfico típico para detectar, informar y prevenir ataques de DOS de capa 7.
- El WAF debe poder detectar, informar y prevenir ataques de fuerza bruta de Capa 7 (capa de aplicación) para intentar ingresar a áreas seguras de una aplicación web al intentar permutaciones exhaustivas y sistemáticas de código o combinaciones de nombre de usuario / contraseña para descubrir una autenticación legítima de credenciales.
- El WAF debe ser capaz de detectar, informar y prevenir el bot web Layer 7 (capa de aplicación) haciendo web scraping recursivo y navegación rápida. También debe tener la capacidad de diferenciar el agente de ataque web automatizado del usuario legítimo. Debe brindar la posibilidad de personalizar la lista predeterminada de motores de búsqueda reconocidos y agregar el motor de búsqueda del sitio a la lista de motores de búsqueda legítimos del sistema.
- El WAF debe poder proporcionar listas blancas de direcciones IP unificadas para las direcciones IP de confianza de Policy Builder y listas blancas de anomalías (Prevención de ataques DoS, Prevención de ataques de fuerza bruta y Detección de web scraping) en una sola lista.
- El WAF debe poder proporcionar un control basado en GUI para determinar la reputación de una dirección IP y operar (por ejemplo, un bloque) basado en esa reputación. La base de datos de reputación de IP se actualiza periódicamente. Detecta la reputación de IP basada en:
 - Explotaciones de Windows
 - Web Attacks
 - Botnets
 - Escáneres
 - Dial de servicio
 - Reputación
 - Proxy de phishing
 - Anxy Proxy
- El WAF debe poder mitigar los vectores DoS que se centran en las debilidades del protocolo HTTP, de los modos:
 - Slow Loris
 - Mensaje lento
 - Hash DoS
 - HTTP Get Flood
- El WAF debe poder detectar ataques DoS al monitorear el número promedio de transacciones por direcciones IP de clientes o URL solicitadas individuales por segundo
- El WAF debe poder detectar los ataques DoS al monitorear el tiempo promedio que tarda el servidor de back-end en responder a una URL específica
- El WAF debe poder detectar, informar y prevenir ataques de fuerza bruta de Capa 7 (capa de aplicación) para intentar ingresar a áreas seguras de una aplicación web al intentar permutaciones exhaustivas y sistemáticas de código o combinaciones de nombre de usuario / contraseña para descubrir una

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:23:41 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:21:01 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:22:18 -05:00

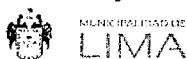


MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

autenticación legítima credenciales.

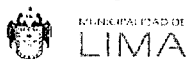
- El WAF debe poder detener a los atacantes no humanos al presentar un desafío de reconocimiento de caracteres a los usuarios sospechosos. Este desafío CAPTCHA se presentará después de que el sistema detecte uno o más de los siguientes problemas:
 - Una dirección IP sospechosa
 - Solicitudes de un país sospechoso.
 - Una URL atacada
 - Un sitio web atacado
- El WAF debe poder mitigar el tráfico de los países que envían tráfico sospechoso.
- El WAF debe poder inyectar un desafío de JavaScript en lugar de la respuesta original para probar si el cliente es un navegador legítimo o un bot.
- El WAF debe poder proteger Web Scraping de los siguientes criterios: detección de bot (actividad de mouse y teclado y detección de navegación rápida), huellas dactilares, clientes sospechosos y apertura de sesión
- El WAF debe ser compatible con la lista blanca de direcciones IP y la lista negra
- El WAF debe tener la capacidad de detectar BOT no basados en navegador como parte de las capacidades de detección de los BOT avanzados de WAF
- El WAF debe poder admitir la aplicación de políticas de seguridad para aplicaciones escritas en el marco del Kit de herramientas web de Google (GWT)
- El WAF debe poder admitir la prevención de enviar o acceder a las cookies cuando el HTTP sin cifrar es el transporte
- El WAF debe poder mitigar los ataques de click-jacking al indicar a los navegadores que no carguen una página en un marco
- El WAF debe poder admitir un escáner genérico a través de un esquema XML publicado
- El WAF debe poder mitigar los Bots a través de Captcha (muro de inicio de sesión). CAPTCHA bajo un ataque de DOS proporciona otra forma de mitigar los BOT. Presenta a los usuarios desafíos de reconocimiento de caracteres para verificar que son humanos. El desafío incluirá letras y dígitos que cambian aleatoriamente. CAPTCHA solo se enviará a intrusos y no a usuarios legítimos.
- El WAF debe ser capaz de detectar patrones de tráfico anómalos que se derivan de una ubicación geográfica única específica y permitir el triangulamiento del tráfico anómalo mediante la ubicación geográfica basada en los conteos de RPS.
- El WAF debe ser capaz de proporcionar una protección siempre activa que evite que los ataques de bots que provocan los ataques de DOS de Layer7, el webscrap y los ataques de fuerza bruta se lleven a cabo. Trabaja con las detecciones de anomaly reactivas existentes. Intenta el desafío de javascript para ralentizar las solicitudes y distinguir los bots antes de que las solicitudes lleguen a un servidor.
- El WAF debe ser capaz de proporcionar ofuscación a JS y seguridad del lado del cliente. Adición de un mecanismo de ofuscación para proteger a JS contra exámenes o ingeniería inversa y manipulación. El mecanismo se ejecutará en BIG-IP como un proceso de background de Java que compila y confunde el código JS, cifrando el código. Esta mejora en última instancia ocultará información confidencial con JS, insertará datos modificables en archivos JS y permitirá un mecanismo de bloqueo sin sincronización de datos generados dinámicamente, incluidos los pares de claves CAPTCHA y RSA.
- El WAF debe poder detectar y mitigar automáticamente los ataques DoS L7 utilizando el aprendizaje automático
- El WAF debe poder admitir la función Anti-bot que evita que el malware pueda robar datos en dispositivos móviles. Detectando bots y clasificando clientes,

Firma digital



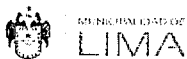
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V - B
Fecha: 17.05.2021 15:24:52 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Fior De
Liz FAU 20131380951 soft
Motivo: Day V - B
Fecha: 15.05.2021 18:21:17 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V - B
Fecha: 15.05.2021 15:21:53 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Identificando el comportamiento humano en dispositivos móviles

- Debe poder visualizar datos históricos de log, eventos, incidencias, análisis de tráfico por un tiempo mínimo de un año de antigüedad, así como poder hacer la importación en formato CSV y pdf.

Estándares de red

- Soporte VLAN 802.1q, Vlan tagging
- Soporte de 802.3ad para definición de múltiples troncales
- Soporte de NAT, SNAT
- Soporte de IPv6: La solución debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
- Soporte de Rate Shapping.
- Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
- Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.
- Debe soportar el protocolo de OVSDb (Open vSwitch Database) para crear tuneles VXLAN usando un controlador SDN
- Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS

Administración del sistema

- La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
- La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
- La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
- La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
- La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
 - Protocolo SysLog
 - Notificación vía SMTP
 - SNMP versión 2.0 o superior.
- El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
- El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
- La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
- Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
- Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:25:56 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:21:42 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:21:34 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

5.2. ALCANCES

La Municipalidad Metropolitana de Lima requiere contratar un servicio de Internet con contingencia y seguridad gestionada, de acuerdo lo descrito en el presente documento.

5.2.1 CONFIGURACIÓN Y SOPORTE TÉCNICO

5211 Configuración

La implementación del servicio constará de la configuración de los equipos involucrados en el servicio de acceso corporativo a Internet y Seguridad Gestionada, para ello, deberá incluir en su propuesta la arquitectura de seguridad tomando en cuenta la actual configuración y mejora de la configuración de los equipos de seguridad instalados en la MML. Dicha información deberá ser obtenida mediante una visita técnica a las instalaciones de la MML.

5212 Mantenimiento Preventivo

Con posterioridad al otorgamiento de la conformidad por la culminación de la implementación y la puesta en operación del servicio, el contratista ganador de la buena pro realizará el mantenimiento preventivo de los equipos que forman parte del servicio, una (1) vez por año, durante todo el periodo de garantía sin interrupción de los servicios.

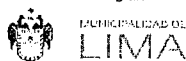
El servicio de mantenimiento preventivo comprenderá las siguientes actividades:

- Configuración y/o Reconfiguración de los equipos involucrados en el servicio de ser necesario algún cambio o mejora que se requiera.
- Afinamiento de la configuración de los equipos.
- Actividades de limpieza interna o externa de los equipos de propiedad del proveedor, que se considere necesario.
- El horario y días para realizar este mantenimiento preventivo, será coordinado previamente con la Subgerencia de Gobierno Digital e Innovación de la MML.
- Finalmente, el proveedor realizará las pruebas de operación en conjunto con el personal técnico de la MML y presentará el informe del servicio, para su conformidad.
- El mantenimiento preventivo también incluye la actualización de las versiones del software suministrados. Por actualización de las versiones se entiende que la Municipalidad Metropolitana de Lima, tenga acceso a las nuevas versiones del software suministrados. La instalación de las nuevas versiones de software se realizará por el contratista, previa coordinación y a solicitud de la MML, todo cambio de configuración, reconfiguración y /o actualización que se requiera para los equipos del servicio no representará costos adicionales para la MML.

5.2.13 Mantenimiento correctivo

- Se entenderá por avería a una interrupción parcial o total del funcionamiento de un equipo.
- La reparación de los equipos incluye el mantenimiento correctivo de averías.
- Si cualquier componente o equipo quedará inoperativo, o mantuviera un funcionamiento defectuoso hasta en tres (03) ocasiones durante un periodo de ciento veinte (120) días calendarios; en cualquiera de ambos casos, el proveedor deberá reemplazar dicha parte o bien, por otro igual o de mejores características, sin costo alguno para la MML.
- Cambio de partes y reconfiguración de los mismos para posibilitar el correcto funcionamiento del equipo.
- Las partes que necesiten ser reemplazados se harán por partes nuevas. (El costo de cualquier solicitud de reconfiguración de los equipos que formaran parte de la propuesta del contratista para los puntos c, d y e) de la presente sección, serán asumidas por el contratista siempre y cuando sea por causas imputables al contratista o se relacione con alguna configuración necesaria para el cumplimiento del servicio y

Firma digital



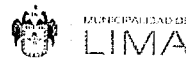
Firmado digitalmente por PARRA
WILLIAMIS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:27:12 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:22:02 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:21:11 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

que no se realizó durante la etapa de implementación del mismo).

- f. Si el equipo no aplica la funcionabilidad de alguna configuración de seguridad o acceso como parte de la seguridad gestionada del presente servicio, el equipo deberá ser reemplazado por uno nuevo de igual o mejores características del equipo propuesto. El tiempo de reemplazo será de cincuenta (50) días calendarios, contados a partir de la elaboración del informe técnico del área usuaria hacia el contratista.
- g. Atención y soporte técnico on-site, según sea el caso o la intensidad del problema presentado.
- h. Las solicitudes para realizar el mantenimiento correctivo al equipo, se llevará a cabo una vez que se reporte la avería, mediante una llamada telefónica o un email, al contratista de acuerdo con el numeral 5. 2. 4.1 Mecanismos para la atención de averías
- i. Toda actividad o provisión de bienes que tenga que ejecutar el contratista ganador de la buena pro para subsanar la avería, se realizará sin costo para la MML.
- j. Todos los servicios derivados de las presentes especificaciones técnicas se deberán respetar y cumplir los tiempos de respuesta máximos establecidos en el presente documento.
- k. Atención de requerimientos o incidentes técnicos bajo la modalidad 24x7x365.

Nivel de servicios

Con posterioridad al otorgamiento de la conformidad por la culminación de la implementación del servicio, el contratista brindará el servicio de soporte on-site y el de mantenimiento correctivo, durante todo el periodo de garantía de acuerdo con los siguientes niveles de servicio:

1. Tiempo de Respuesta

Como tiempo de respuesta se define el período desde que se genera el requerimiento del servicio por parte de la MML, hasta el instante en que el técnico designado por el proveedor toma contacto (de acuerdo con el mecanismo de atención a averías) con los técnicos encargados de la MML. Este tiempo de respuesta no excederá de **UNA (01) HORA**. En todos los casos, deberá existir la constancia de que la respuesta del proveedor ha sido recibida por el personal de la MML, para contabilizar los tiempos de respuesta.

2. Tiempo de Solución (TS)

Se define como tiempo de solución, al período desde que se genera el requerimiento del servicio por parte de la MML, hasta el instante en que el técnico designado por el proveedor deje correctamente operativo el equipo, sistema o accesorio u otro, por el cual, el servicio resultó afectado. Este tiempo de solución será de hasta **CUATRO (04) HORAS** cronométricas **COMO MAXIMO**, **OCHO (08) HORAS** para el caso de rotura de una fibra, y para el caso de desastres naturales o similares el tiempo será evaluado por las partes.

De ser necesario el retiro del equipo, el proveedor deberá dejar un equipo de iguales o mejores características debidamente configurado y operativo en la MML, hasta que solucione definitivamente el problema en el bien reportado con falla. Dicha falla deberá solucionarse en los próximos **50 DÍAS CALENDARIOS** como máximo, de lo contrario el proveedor realizará un cambio del equipo en el 51avo día. Este cambio deberá ser por un equipo o parte nuevos de igual o mejores prestaciones bajo la conformidad de la SGDI de la MML, sin que este represente costo adicional para la MML.

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:28:28 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SCLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:22:23 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:20:49 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

El incumplimiento de los SLA está sujeto a penalidades.
Todas las incidencias deber informadas por correo, independientemente de que deben ser incluidas en el informe mensual de servicio

3. Cobertura Horaria

El horario de atención solicitado se realizará las 24 horas del día, los 7 días de la semana, los 365 días del año, durante la vigencia del contrato.

4. El Nivel de Servicio del sistema (SLA)

Será del 99.90% de disponibilidad de todo el sistema. Se considera una avería a la interrupción parcial o total del servicio de acuerdo al SLA siempre que sea imputable al operador que brinda el servicio. Cabe aclarar que el SLA tiene como objetivo fijar el nivel acordado de la calidad del servicio que la entidad desea recibir. Por tanto, se aclara que se contará con una SLA estándar de disponibilidad del 99.90% con los tiempos de atención y solución de averías solicitadas.

5.2.2 Del Centro de Operación de Red (NOC)

El contratista deberá asegurar el monitoreo permanente del servicio de acceso a Internet y de los aspectos de la seguridad de los datos que circulan por él; para ello el contratista deberá contar con un Centro de Operación de Red (NOC) que realice la gestión de los enlaces (principal y contingencia) y del servicio de Internet, así como también, de la configuración de equipos y servicios a demanda de la MML. Si las funciones comprendidas en la solución se concentran o se dividen en uno o más centros de operaciones, no será una limitante para considerar su cumplimiento en tanto se cumplan los niveles y características de los requerimientos efectuados

5.2.2.1 Características del NOC

El NOC deberá estar en capacidad de realizar acciones de controles preventivos, correctivos y pruebas técnicas que puedan contribuir a analizar, resolver y superar las incidencias que afecten el servicio de acceso a Internet, a fin de garantizar un eficiente funcionamiento del servicio de acceso a Internet y determinar la responsabilidad de las partes en cada caso.

5.2.2.2 Tareas del NOC

- Deberá efectuar un monitoreo permanente del servicio implementado las 24x7x365, así mismo el proveedor será responsable de la actualización oportuna de parches y de hacer las copias de respaldo de las configuraciones y políticas de la solución implementada cuando sea necesario, de no ser así se aplicarán penalidades al contratista del servicio.
- Deberá dar solución a fallas de manera remota o en sitio.
- Un (01) mantenimiento preventivo cada año a los equipos en condición de alquiler, durante el período del contrato, que incluyan las siguientes labores:
 - Revisión del estado físico y lógico de los equipos
 - Limpieza externa de los equipos
- Deberá verificar continuamente los medios de transmisión.
- Durante el período de garantía, deberá reparar o reemplazar sin costo para la MML



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

los equipos o componentes que sean necesarios para asegurar la prestación del servicio, en caso de fallas imputables al contratista.

- f. El contratista deberá brindar la facilidad de acceso a todos los equipos que forman parte del servicio, a los miembros del personal técnico designado por la MML, de forma local o remota a través de usuarios con perfil de "sólo lectura"; para labores de monitoreo, revisión general del estado del equipo (contadores, uptime, versión de firmware, revisión de eventos). Se crearán hasta dos usuarios para el personal de la SGDI de la MML.
- g. El NOC deberá ser la primera fuente de información hacia el área usuaria sobre ataques o alteraciones al servicio de internet (información mediante correos y/o llamada telefónica).
- h. Durante la vigencia del contrato, deberá entregar dentro de los primeros cinco días hábiles de cada mes los reportes de las fallas ocurridas durante el servicio del mes precedente, de acuerdo a la siguiente clasificación:
- Relación de incidencias de seguridad, intentos de intrusión y/o ataques de seguridad ofensiva, en el mes precedente.
 - Reporte detallado de fallas y su tiempo de solución, donde se refleje el número de horas sin servicio imputables al proveedor y los imputables a la MML o a causas de fuerza mayor en el sitio afectado.
 - Reportes atendidos con proactividad y los generados por la MML.
 - Reportes de desempeño de equipos, servicios y aplicaciones, especificando:
 - Utilización de CPU
 - Utilización de memoria
 - Utilización de ancho de banda
 - Se considerará válido que los reportes sean realizados por el personal técnico asignado por el proveedor, así mismo deberá notificar el reporte realizado al personal designado por la MML.
- i. El contratista del servicio deberá entregar informes detallados que serán requeridos a demanda, o en su defecto, deberá entregar el procedimiento que el personal encargado de la MML deberá realizar para obtener la información requerida para la administración de las fallas del servicio:
- Relación de incidencias de seguridad, intentos de intrusión y/o ataques de seguridad ofensiva.
 - Fecha y hora de la última alarma del sitio.
 - Tiempo promedio de solución y respuesta.
 - Relación de incidencias / reincidencias del mes.
 - Clasificación de reportes por tipo de falla.
 - Frecuencia y tipo de fallas.
 - Identificación de problemas.
 - Plan de acción para corregir desviaciones en los niveles de servicio.
 - Tiempo promedio de solución y respuesta.
 - Casos abiertos y cerrados.
 - Proactividad: casos proactivos, casos reactivos (en porcentaje y gráfica).
 - Además, deberá entregar un resumen ejecutivo en forma impresa, donde sintetice las labores del NOC y del SOC (resumen de actividades), incluyendo el control de los cambios en las configuraciones de los equipos involucrados, requeridos para mantener los niveles de servicio, además del resumen de las siguientes variables del rendimiento de sus equipos y servicios:
 - Disponibilidad del enlace del servicio de Internet.
 - Utilización de CPU.
 - Utilización de memoria.
 - Utilización de ancho de banda del servicio de internet.
- j. El resumen ejecutivo solicitado deberá ser presentado a demanda de la MML.
- k. Se requiere que el monitoreo del enlace contratado considere los siguientes aspectos:
- Consumo de ancho de banda en tiempo real.

○

○

Firma digital
MUNICIPALIDAD DE LIMA
Firmado digitalmente por PARRA WILLIAMS Ruben Emilio FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:30:22 -05:00

Firma digital
MUNICIPALIDAD DE LIMA
Firmado digitalmente por HUAYHUA SOLORZANO Flor De Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:22:54 -05:00

Firma digital
MUNICIPALIDAD DE LIMA
Firmado digitalmente por MANTILLA LEON Richard Jean Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:20:05 -05:00

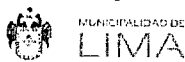


MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACION

- Visualización de enlace en línea y tuera de servicio.
 - Utilización del ancho de banda.
 - Notificación de los problemas en la red y/o los equipos.
- l. El contratista del servicio deberá entregar en formato Excel el comportamiento mensual del uso de ancho de banda por tipo de uso y por usuario debiendo capacitar a 2 personas designadas por la MML para que puedan hacerlo en paralelo y en forma independiente.
- m. El contratista de la buena pro deberá publicar una Página web en donde se pueda visualizar on-line, información de la disponibilidad del enlace, ocupación del ancho de banda, tráfico de los protocolos (ftp, http, e-mail), en forma gráfica correspondiente a los enlaces contratados. La herramienta de generación de reportes de forma gráfica deberá guardar un histórico de la información solicitada, por al menos 6 meses. Queda bajo criterio del contratista definir los equipos, tecnologías, herramientas y/o Procedimientos a utilizar para cumplir con este requerimiento. La herramienta de monitoreo web utilizada por el proveedor no deberá impactar en el ancho de banda. El sistema de monitoreo deberá contar con la capacidad de graficar y emitir reportes de los indicadores (ancho de banda; tráfico por protocolos ftp, http, e-mail; disponibilidad del enlace) monitoreados por día, semana, y de manera mensual. La MML se reserva la potestad de verificar la información presentada por el contratista, ya sea mediante visitas al NOC del contratista a fin de constatar los informes de rendimiento emitidos por el contratista o mediante herramientas de control propias.
- n. Deberá proporcionar el acceso a la herramienta de monitoreo Web, para dos (02) personas designadas por la MML, con el fin de que éstas puedan monitorear en línea el consumo de ancho de banda, disponibilidad de los servicios y alarmas.
- o. Deberá dar acceso al personal de la MML (02 cuentas) a la herramienta de monitoreo web para permitir la verificación de la actividad de los enlaces.
- p. Queda bajo criterio del contratista definir los equipos, tecnologías, herramientas y/o procedimientos a utilizar para cumplir con estos requerimientos.
- q. Los informes diarios, que son por incidencias o eventos presentados durante el servicio de acceso a Internet, deberán contener la hora de inicio y fin de la incidencia, el diagnóstico del problema, el tiempo estimado de solución y las actuaciones realizadas por el contratista para dar solución al problema. Estos informes se entregarán como parte de una bitácora de incidencias del día, de los casos cerrados, pendientes y por apertura. Estos informes deberán ser entregados al final del día.

5.2.3 Del Residente

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:31:17 -05:00

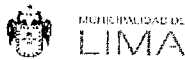
Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:23:15 -05:00

- a) El personal técnico asignado por el proveedor a la MML para el servicio de acceso a Internet con seguridad gestionada se encargará de observar el desempeño de todos los equipos, realizar las bitácoras que serán enviadas al final del día, alarmas, eventos y reportes.
- b) El monitoreo solicitado deberá ser de responsabilidad del contratista, y deberá ser realizado por el personal técnico asignado por el contratista, con la supervisión del personal de la MML.
- c) Cuando la herramienta de monitoreo permanente o el personal asignado por el proveedor detecte los problemas de falla en la red y/o en los equipos informará sobre la misma, vía correo electrónico o telefónicamente, al personal designado por la MML. De ser necesario, la MML generará un reporte de averías al centro de gestión del contratista.
- d) Canalizará las solicitudes de configuraciones a fin de mejorar el servicio a iniciativa de la Entidad o recomendación del contratista sin que estas generen costos para la Entidad. Las actividades de configuraciones para mantener óptimo el servicio son dinámicas y constantes.

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:19:14 -05:00

5.2.4 De la atención de averías.

- a. Se entenderá por avería a una interrupción parcial o total del servicio, así como a una pérdida de la calidad de este.



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

- a. Toda actividad o provisión de bienes que tenga que ejecutar el contratista de la buena pro para subsanar la avería y continuar con la prestación del servicio se realizará sin costo para la MML.
- b. Se entenderá como tiempo de respuesta, al tiempo transcurrido entre la identificación de la falla hasta la generación del ticket de atención solicitada por la entidad
- c. Se entenderá por tiempo de subsanación, al tiempo transcurrido entre la comunicación de la MML al contratista ganador de la buena pro de la existencia de una avería y la subsanación de esta a satisfacción de la MML.
- d. La MML podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas.
- e. Las llamadas de servicio se sujetarán a lo siguiente:

- Se podrán efectuar telefónicamente a los números telefónicos indicados por el contratista.
- La MML a través del área usuaria mediante un correo notificará las anomalías que se presenten incluyendo la siguiente información: fecha, hora, descripción del problema y nombre del contacto en la MML.

- f. El tiempo de respuesta y diagnóstico de una avería que afecte el servicio, ante una llamada formulada por la MML, no deberá exceder de 1 hora a partir de la llamada o comunicación efectuada por la MML.
- g. El tiempo de subsanación total de la avería o caída del enlace de internet no deberá exceder de 4 horas a partir de la hora de la notificación, a excepción de los siguientes casos:
- Rotura de fibra en los cuales el tiempo de subsanación será de 8 horas.
 - Desastres naturales u otros casos de igual consideración en los cuales el tiempo de subsanación será evaluado por ambas partes.
- h. Entretanto se subsane completamente la avería o caída del enlace, independientemente de la complejidad de la solución al problema, el enlace de contingencia deberá entrar en operación en forma inmediata de forma tal que no se afecte el servicio de acceso a Internet, dentro de los niveles de disponibilidad de los enlaces del servicio de Internet exigidos (99.90%).
- i. En ausencia del personal de la MML, el Centro de Operación de Red (NOC) deberá realizar el reporte de la avería a fin de que se atienda oportunamente. El NOC deberá estar disponible para el diagnóstico y atención de averías los 7x24x365.
- j. El cierre de un reporte de fallas debe realizarse de manera coordinada entre el personal del proveedor y el personal técnico designado por la MML. El reporte generado, sólo podrá ser cerrado cuando sea corroborada la solución de la falla y aceptada con el visto bueno del personal designado por la MML.

5. 2. 4.1 Mecanismos para la atención de averías

Con la finalidad de establecer un canal directo de atención entre el NOC del contratista ganador de la buena pro y los encargados de comunicaciones de la MML, que permita reducir los tiempos de atención de averías y mantener permanente coordinación durante los procesos de atención y cierre de averías.

El contratista deberá proveer los mecanismos y/o procedimientos conteniendo como mínimo el número de teléfono y correo al cual se comunicará la entidad para la atención de averías, así como acceso a la herramienta web, a los encargados de la MML, para realizar el monitoreo permanente del servicio. Queda bajo criterio del contratista definir los equipos, tecnologías, y/o herramientas a utilizar para cumplir con este requerimiento.

El contratista deberá contar con un Call Center Técnico y con números de emergencia para reportar los servicios y averías.

El costo generado por este requerimiento deberá ser asumido en su integridad por el contratista ganador de la buena pro durante el período de prestación del servicio de acceso a Internet.



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

5.3. IMPLEMENTACION DEL SERVICIO

5.3.1 Plan del proyecto.

Dentro de los cuatro (4) días calendarios siguientes de la suscripción del contrato, el contratista ganador de la buena pro deberá entregar:

- Plan del Proyecto: análisis, diseño, descripción de actividades, fechas de la implementación del proyecto.
- Cronograma de instalación, pruebas protocoladas y puesta en operación.

Las pruebas protocoladas deben contener el detalle de los protocolos de pruebas a realizar, para confirmar que cada uno de los equipos y servicios implementados cumplan con los niveles de servicios requeridos.

El Plan del proyecto será aprobado por el área técnica de la Subgerencia de Gobierno Digital e Innovación mediante un acta en un plazo máximo de tres (03) días calendarios a partir del día siguiente de la entrega del Plan de proyecto y será suscrito por el área técnica de la Subgerencia de Gobierno Digital e Innovación.

5.3.2 Implementación

El contratista debe tomar un tiempo máximo de sesenta (60) días calendario para la implementación, a partir del día siguiente de suscrito el acta de la aprobación del Plan del proyecto.

Culminada la implementación se suscribirá un acta de culminación de implementación del servicio, suscrito por el área técnica de la Subgerencia de Gobierno Digital e Innovación.

5.3.3 Inspección

El contratista ganador de la buena pro y el personal de la MML, una vez terminada la implementación del servicio, realizarán en forma conjunta los procedimientos de inspección y pruebas protocoladas sobre la infraestructura y equipos instalados, de tal forma que, les permita establecer que los servicios sean brindados de conformidad con lo solicitado en los presentes términos de referencia y en la propuesta del contratista.

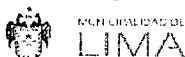
La inspección tendrá como plazo máximo de siete (7) días calendarios, contados a partir del día siguiente de suscrito el Acta de culminación de la implementación del servicio.

Las pruebas se realizarán en las sedes de la MML. Los costos que demanden las mismas no implicarán en ningún caso reconocimiento de gastos y deberán ser provistos por el contratista.

La omisión de algún componente técnico, que al momento de las pruebas resulte necesario para la provisión del servicio o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al contratista a proveerlo sin costo adicional.

Cualquier defecto imputable al contratista durante la realización de las pruebas de aceptación, deberá ser corregido por éste, sin costo alguno.

Firma digital



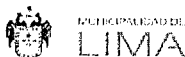
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:35:35 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:23:55 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:18:55 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Una vez realizados los procedimientos de inspección y pruebas, a satisfacción de la MML, se levantará un Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio.

5.3.4 Inicio del servicio

El inicio del servicio se producirá al día siguiente de la fecha de suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio, la cual será suscrita por el contratista y la Subgerencia de Gobierno Digital e Innovación de la Gerencia de Administración de la MML. La suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio debe ser realizada al final del periodo de inspección, el cual dura 07 días

5.4. MEDIDAS DE SEGURIDAD A ADOPTARSE

El Contratista deberá cumplir todas las medidas de seguridad y todas las referidas a la Ley 29783 Ley de Seguridad y Salud en el Trabajo y su Reglamento, siendo causal de la aplicación de las penalidades descritas la no observancia de alguna de las normas y/o medidas contempladas en dichos documentos.

✓ Seguros

El contratista deberá contar con todos los seguros complementarios de trabajo de riesgo vigente, para todo el personal que participará en la implementación y ejecución del servicio.

✓ Indumentaria y equipos de protección personal

Durante la implementación y ejecución del servicio, el personal deberá presentarse aseado y con la siguiente indumentaria mínima: pantalón, polo, zapato cerrado y/o bota y fotocheck de identificación.

✓ Medidas sanitarias por el COVID-19

Durante la implementación y ejecución del servicio, el contratista es responsable, de realizar sus actividades aplicando estrictamente los protocolos sanitarios y demás disposiciones que dicten los sectores y autoridades competentes, para la prevención, contención y mitigación del COVID-19, que resulten aplicables de acuerdo con la naturaleza de su actividad.

Durante la implementación y ejecución del servicio, el contratista deberá contar y usar obligatoriamente con los siguientes equipos de protección personal: mascarillas que cubran boca y nariz, protector facial y protección adicional necesaria que contemple la normativa aplicable para la prevención de contagio del virus que ocasiona el COVID- 19

El contratista está obligado a cumplir con los requisitos legales en materia de seguridad y salud ocupacional aplicables a sus actividades y de acuerdo con la normatividad vigente.

5.5. LUGAR Y PLAZO DE PRESTACION DEL SERVICIO

5.3.5 LUGAR:

Subgerencia de Gobierno Digital e Innovación ubicada en el 3er piso de la Municipalidad Metropolitana de Lima, calle Jr. Conde de Superunda N° 141, Lima Cercado – ubicación de los equipos (3er piso).



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

5.3.6 PLAZO DE IMPLEMENTACIÓN

El plazo máximo será **74 DÍAS CALENDARIOS** contados a partir del día siguiente de la suscripción del contrato.

5.3.7 PLAZO DEL SERVICIO:

El tiempo de prestación de los servicios será de **TREINTA Y SEIS (36) MESES** contados a partir de la suscripción del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio.

5.6. ENTREGABLES

Plan del Proyecto

El contratista ganador, dentro de los cuatro (4) días calendario contados a partir del día siguiente de la suscripción del contrato, entregará: Análisis, diseño, descripción de actividades, fechas de la implementación del proyecto, Cronograma de instalación, pruebas protocoladas y puesta en operación del servicio.

Las pruebas protocoladas deben contener el detalle de los protocolos de pruebas a realizar, para confirmar que cada uno de los equipos y servicios implementados cumplan con los niveles de servicios requeridos.

Informe Técnico de Implementación del servicio

El contratista deberá presentar los entregables definidos en este documento en tres (03) copias impresas y en tres (03) CDs o medio magnético. Los entregables deberán incluir el Informe Final de la Implementación del Servicio en la mesa de partes de la Entidad.

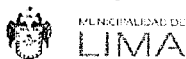
El informe debe contener los detalles de la implementación del servicio y como mínimo lo siguiente:

- c) Planos del recorrido de las rutas y ubicación de los nodos que se utilizarán para el enlace principal y los que se utilizarán para el enlace secundario; y protocolo de pruebas para la verificación del recorrido de las rutas y ubicación de los nodos utilizados para los enlaces principal y secundario.
- d) Archivo de configuración de todos los equipos instalados.
- e) Diseño de la Arquitectura y Topología del servicio propuesto.
- f) Manuales técnicos y de usuario de los equipos instalados, el cual podrá ser presentado al final de la implementación del proyecto (Se precisa que estos se refieren a los brochures, datasheets y manuales de configuración).
- g) Protocolos de pruebas.
- h) Documentación de la ejecución del proyecto conteniendo los reportes de las pruebas protocoladas, entre otros.
- i) Diagrama de red y topología de la implementación de la solución de internet donde se muestre los equipos de redundancia, seguridad y gestión de los mismos.
- j) Diseño de la ruta del enlace principal y del enlace secundario.

Los documentos se deberán entregar en formato electrónico (MS Office). En tres ejemplares, impresos y en medio óptico, por mesa de partes de la Entidad

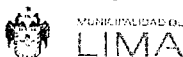
La entrega del informe final del contratista será con un plazo máximo de tres (3) días calendarios contados desde el día siguiente del Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio.

Firma digital



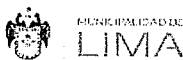
Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V. B.
Fecha: 17.05.2021 15:37:54 -05:00

Firma digital



Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V. B.
Fecha: 15.05.2021 18:24:33 -05:00

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Joan
Paul FAU 20131380951 soft
Motivo: Doy V. B.
Fecha: 15.05.2021 15:16:59 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Informe Técnico Servicio de Internet (Mensual)

Para efectos de obtener las conformidades mensuales deberá presentar los Informes Técnicos mensuales conteniendo, como mínimo, los reportes siguientes:

- Relación de incidencias de seguridad, intentos de intrusión y/o ataques de seguridad ofensiva, en el mes precedente.
- Reporte detallado de fallas y su tiempo de solución, donde se refleje el número de horas sin servicio imputables al proveedor y los imputables a la MML o a causas de fuerza mayor en el sitio afectado.
- Reportes atendidos con proactividad y los generados por la MML.
- Relación de incidencias / reincidencias del mes.
- Clasificación de reportes por tipo de falla.
- Frecuencia y tipo de fallas.
- Casos abiertos y cerrados.
- Trabajos relevantes del Ingeniero Residente
- Reportes de desempeño de equipos, servicios y aplicaciones, especificando:
 - Utilización de CPU
 - Utilización de memoria
 - Utilización de ancho de banda
- Nivel de disponibilidad del Servicio en el mes precedente.

Estos últimos deberán entregarse en 2 copias impresas y en dos (02) CDs o medio magnético en la mesa de partes de la Entidad con un máximo de 10 días siguientes de terminado el periodo mensual del servicio de internet.

5.7. SISTEMA DE CONTRATACIÓN:

Suma Alzada.

5.8. GARANTÍA DEL SERVICIO:

El contratista se comprometerá a garantizar el trabajo realizado como parte del mantenimiento correctivo y preventivo efectuado, sin costo adicional alguno para la Entidad, por un periodo de 36 meses.

a. **ALCANCE DE LA GARANTÍA:** Tres (03) años, contra defectos de diseño y/o fabricación, averías, fallas o desperfectos de funcionamiento y o configuraciones no aplicables de los equipos e instalación no detectable al momento que se otorgó la conformidad del servicio y durante el tiempo que dure la garantía.

b. **INICIO DE GARANTIA:** Desde el día siguiente de otorgada la conformidad del servicio.

6. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1. DEL PERSONAL CLAVE

Un (01) Jefe de Proyecto

FORMACIÓN ACADÉMICA

Con título en Ingeniería en Electrónica, Ingeniería Industrial, Telecomunicaciones,



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACION
informática, Computación o Sistemas.

EXPERIENCIA

El jefe de proyectos deberá contar con experiencia mínima de cuatro (04) años como Jefe de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.

CAPACITACIONES

Certificado o Diplomado como Profesional en Project Management. El contratista deberá documentar lo solicitado.

ACTIVIDADES:

Gestionar todo el proyecto desde el inicio hasta la puesta en marcha del servicio requerido

Un (01) Supervisor

FORMACIÓN ACADÉMICA

Con Bachiller o título en Ingeniería Electrónica, Ingeniería Industrial, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Computación y Sistemas

EXPERIENCIA

El supervisor deberá contar con experiencia mínima de cuatro (04) años como jefe o supervisor de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.

CAPACITACIONES

Certificado en la marca propuesta como asociado o profesional o experto en routing y/o switching y/o firewalling, el mismo que deberá estar vigente o activo (comprobable en base a una referencia on-line o certificada del fabricante), se deberá indicar dicha referencia y el código del certificado para su verificación. El contratista deberá documentar lo solicitado.

ACTIVIDADES: Supervisar cada una de las actividades a ejecutar en las fases de proyecto desde el inicio hasta la puesta en marcha del servicio requerido

Personal técnico

Técnico Perfil 1 (2 Personas)

FORMACIÓN ACADÉMICA

Profesional técnico en redes y comunicaciones o Sistemas o informática o electrónica y/o Bachiller o titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería electrónica o Ingeniería Industrial o Ingeniería de Telecomunicaciones.

EXPERIENCIA

Dos (02) personas, que deberán tener dos (02) años de experiencia en actividades de routing y switching

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:39:56 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLORZANO Flor De
Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:25:13 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:16:17 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN
CAPACITACIONES



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 solt
Motivo: Doy V° B°
Fecha: 15.05.2021 15:15:53 -05:00

Certificación en nivel de asociado, especialista o profesional en routing y switching de la marca propuesta.

Actividades: Instalación y configuración de los equipos de red y/o comunicaciones que son componentes del servicio requerido

Técnico Perfil 2 (2 Personas)

FORMACIÓN ACADÉMICA

Profesional técnico en redes y comunicaciones o Sistemas o informática o electrónica y/o Bachiller o titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería electrónica o Ingeniería Industrial o Ingeniería de Telecomunicaciones.

EXPERIENCIA

Dos (02) personas, que deberán tener dos (02) años de experiencia en actividades de firewalling

CAPACITACIONES

Certificación de especialista o profesional en firewalling de la marca propuesta.

ACTIVIDADES: Instalación y configuración de seguridad que son componentes del servicio requerido

Técnico Perfil 3 (2 Personas)

FORMACIÓN ACADÉMICA

Profesional técnico en redes y comunicaciones o Sistemas o informática o electrónica y/o Bachiller o titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería electrónica o Ingeniería Industrial o Ingeniería de Telecomunicaciones.

EXPERIENCIA

Dos (02) personas, que deberán tener dos (02) años de con experiencia en Administradores de Ancho de Banda de la marca propuesta.

ACTIVIDADES: Instalación y configuración de los equipos de balanceo y distribución de ancho de banda que son componentes del servicio requerido

Es preciso indicar que:

- Una persona puede tener más de 1 certificado requerido
- En el caso de certificados deberán estar vigente o activo (comprobable en base a una referencia on-line o certificada del fabricante), se deberá indicar dicha referencia y el código del certificado para su verificación.

6.2. CONFORMIDAD DE LA PRESTACIÓN:

La conformidad de servicio de internet estará a cargo de la Subgerencia de Gobierno de Digital e Innovación, en el marco del Artículo 168°- Recepción y conformidad del Reglamento de la Ley de Contrataciones del Estado.



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

La conformidad de la implementación del servicio será otorgada luego de recibido la siguiente documentación por parte del contratista:

- Informe de instalación y funcionamiento del servicio, adjuntando documentos indicados en el acápite entregables.

La conformidad de la prestación mensual del servicio luego de recibido lo siguiente por parte del contratista:

- Informe mensual del Servicio contratado
- Comprobante de pago.

6.3. FORMA DE PAGO:

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en forma mensual.

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

- Informe del servicio mensual por parte del área técnica de la Subgerencia de Gobierno Digital e Innovación emitiendo la conformidad de la prestación efectuada. Previo Informe mensual del Servicio contratado emitido por el contratista.
- Comprobante de pago.

La documentación del contratista debe ser dirigida a la Subgerencia de Gobierno Digital e Innovación y se debe presentar en Mesa de Partes de la Municipalidad Metropolitana de Lima.

La MML efectuará los pagos en soles, de la siguiente manera:

- El pago por el concepto del servicio se contabiliza a partir del día siguiente de suscrita el Acta de Conformidad por la culminación de la implementación total y puesta en marcha del servicio. El monto mensual se determinará del 100% del monto adjudicado, el cual se mantendrá fijo y no estarán sujetos a reajuste alguno, durante el periodo de treinta y seis (36) meses.

6.4. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de la prestación objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, en virtud del artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

6.5. OTRAS PENALIDADES

En la fase de ejecución del servicio:

1. Cuadro de Penalidades para el servicio de Acceso a Internet

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:15:34 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:15:16 -05:00

	Porcentaje de disponibilidad de los componentes del servicio de acceso corporativo a Internet:	%
Interrupciones del servicio imputables al contratista (corte parcial, total de los componentes del servicio descritos en el Cuadro de Penalidades)	Medios de transmisión del proveedor.	Deducible de la facturación mensual
	Equipos de comunicaciones del proveedor.	
	Mayor o igual a 99.90%	
	Menor a 99.90% y Mayor o igual a 99.75%	
	Menor a 99.75% y Mayor o igual a 99.50%	
	Menor a 99.50 % y Mayor o igual a 99.00%	0%
	Menor a 99.00% y Mayor o igual a 98.00%	5%
	Menor a 98.00% y Mayor o igual a 97.00%	6%
	Menor a 97.00%	7%
		8%
En caso de aplicarse la penalidad en tres (03) meses consecutivos o seis (06) no consecutivos la entidad podrá resolver el contrato por incumplimiento.		9%
100% = 24 horas x n (n = días del mes. Por ejemplo: en marzo, n=31; en abril, n=30)		20%
Para efectos del cálculo de la penalidad, se acumularán las horas en las que el servicio se haya interrumpido en el mes. Para este cálculo se tomará en cuenta que el 100% equivale al número total de horas mensuales.		

En los casos en que se produzca un retraso en la atención de averías, y el motivo del retraso sea imputable a las gestiones de acceso al local u otras causas atribuibles a la MML, se considerará una "parada de reloj" la cual será registrada por personal de la MML y se reanudará una vez superado el inconveniente a efectos de llevar el control de los tiempos de atención requeridos en los términos de referencia del servicio.

2. Por el incumplimiento de soporte técnico de los SLA la penalidad será la siguiente:

Firma digital
MUNICIPALIDAD DE LIMA
Firmado digitalmente por PARRA WILLIAMS Ruben Emilio FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 17.05.2021 15:42:28 -05:00

Item	Demora de tiempo en solución	Valor de la Penalidad
1	De 1 a 3 horas	20% de una UIT
2	De 4 a 5 horas	60% de una UIT
3	De 6 a 8 horas	80% de una UIT
4	Mayor a 9 horas	70% de una UIT por cada hora de incumplimiento

Otros casos sujetos a penalización se consideran en el siguiente cuadro:

N°	SUPUESTO DE APLICACIÓN DE PENALIDADES	FORMULA DE CALCULO
1	Cuando el contratista realice la rotación y/o reemplazo del personal clave, sin comunicar a la Subgerencia de Gobierno Digital e Innovación.	5 % de UIT por cada ocurrencia
2	Cuando el Contratista incumpla con el cambio de equipo ya sea por falla de fabricación o desperfecto del equipo o porque no aplique configuraciones de seguridad o funcionalidad que sean necesarias para el servicio.	10% de la UIT por cada día pasado el tiempo de solución.
3	Cuando el contratista no cumpla con el traslado del servicio secundario y el traslado y configuración de los equipos de seguridad gestionada a otra sede que requiera el área usuaria.	10 % de la UIT por cada día de retraso

Firma digital
MUNICIPALIDAD DE LIMA
Firmado digitalmente por HUAYHUA SOLOZANO Flor De Liz FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 18:26:15 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

4	Cuando el contratista no cumpla con el plazo establecido para la implementación del servicio	10 % de la UIT por cada día de retraso
---	--	--

PROCEDIMIENTO

La SGDI, al advertir el incumplimiento, levantará un informe el cual será comunicado a la Subgerencia de Logística Corporativa para la aplicación de penalidad respectiva.

6.6. RESPONSABILIDAD POR VICIOS OCULTOS:

La recepción conforme de la prestación 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 artículo 173° de su Reglamento. Por lo que el Contratista será responsable por la calidad ofrecida y por los vicios ocultos por un plazo de tres (3) años contado a partir de la conformidad otorgada por la MML.

6.7. DOCUMENTOS PARA LA SUSCRIPCIÓN DEL CONTRATO

Además de los documentos señalados en las bases administrativas del procedimiento de selección el contratista adjudicado deberá presentar los siguientes documentos para la suscripción del contrato:

- Nombre completo de la persona de contacto, números de teléfonos y correos electrónicos para las coordinaciones durante la ejecución contractual.
- Pólizas de seguros SCTR del personal clave.
- Nombres y documentos de identificación del personal clave propuesto.
- Certificado de antecedentes penales y policiales del personal clave propuesto.
- Certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS a fin de asegurar el cumplimiento de las especificaciones de IPv6 y que puedan funcionar de manera segura sin inconvenientes.
- El contratista deberá presentar una carta del fabricante indicando que la solución implementada para brindar el servicio Anti-DDoS se encuentra con vigencia tecnológica a fin de que la protección de la red de la Entidad este actualizada en cuando las últimas modalidades y tipos de ataques.

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:14:50 -05:00

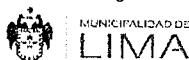
Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por
HUAYHUA SOLOZANO Flor De
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:26:36 -05:00

Firma digital



MUNICIPALIDAD DE
LIMA

Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:43:19 -05:00



REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El contratista debe acreditar un monto facturado acumulado equivalente a S/ 3,500 000.00 (Tres Millones Quinientos Mil 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.</p> <p>Se consideran servicios similares a los siguientes:</p> <ul style="list-style-type: none">• Servicio de Transmisión de Datos mediante fibra óptica• Transmisión de datos a través de red privada virtual• Transmisión digital o de comunicaciones digitales• Servicio de seguridad de red,• Servicio de seguridad perimetral• Servicio de Internet• Servicios de transmisión de dato. <p><u>Acreditación:</u></p> <p>La experiencia del contratista 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 pago¹, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los Contratistas 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 referido a la Experiencia del Contratista en la Especialidad.</p> <p>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.</p> <p>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.</p> <p>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 de que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p>

¹ Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

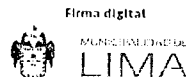
"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio contratista, no puede ser considerado como una acreditación que produzca fehacencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del contratista afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del contratista [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".



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:14:19 -05:00

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

Si el contratista acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo referido**.

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 Contratistas deben llenar y presentar el **Anexo** referido a la Experiencia del Contratista en la Especialidad.

Importante

- *Al calificar la experiencia del contratista, se debe valorar de manera integral los documentos presentados por el contratista 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 contratista 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".*

B CAPACIDAD TÉCNICA Y PROFESIONAL

B.3 CALIFICACIONES DEL PERSONAL CLAVE

B.3.1 FORMACIÓN ACADÉMICA

Un (01) Jefe de Proyecto:

Con título en Ingeniería en Electrónica, Ingeniería Industrial, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Computación y Sistemas.

Un (01) Supervisor

Con Bachiller o título en Ingeniería Electrónica, Ingeniería Industrial, Ingeniería de Telecomunicaciones, Ingeniería Informática, Ingeniería de Computación y Sistemas

Seis (6) Técnicos para la implementación del servicio.

Profesional técnico en redes y comunicaciones o Sistemas o informática o electrónica y/o Bachiller o titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería electrónica o Ingeniería Industrial o Ingeniería de Telecomunicaciones.

Acreditación:

El título profesional o el Grado de bachiller, será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, 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 : <http://www.titulosinstitutos.pe/>, según corresponda.

En caso el título profesional o el Grado de bachiller, 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.3.2 CAPACITACIÓN

Requisitos:

Un (01) Jefe de Proyecto:

Firma digital



Firmado digitalmente por
HUAYHUA SOLOZANO Flor Ds
Lic FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 18:27:22 -05:00

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Ruben Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:48:37 -05:00



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Doy V° B°
Fecha: 15.05.2021 15:14:04 -05:00

~~Certificado o Diplomado como Profesional en Project-Management. El contratista deberá documentar lo solicitado.~~

UN (01) Supervisor

Certificado en la marca propuesta como asociado o profesional o experto en routing y/o switching y/o firewalling, el mismo que deberá estar vigente o activo (comprobable en base a una referencia on-line o certificada del fabricante), se deberá indicar dicha referencia y el código del certificado para su verificación. El contratista deberá documentar lo solicitado.

Dos (02) Técnico Perfil 1

Certificación de especialista o profesional en routing y switching de la marca propuesta.

Dos (02) Técnico Perfil 2

Certificación de especialista o profesional en firewalling de la marca propuesta.

Acreditación:

Se acreditará con copia simple de constancias, y/o certificados y/o diploma

Importante

Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.

B.4 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

Un (01) jefe de Proyecto

Con cuatro (04) años como Jefe de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.

Un (01) supervisor

El supervisor deberá contar con experiencia mínima de cuatro (04) años como jefe o supervisor de Proyecto en Proyectos de Implementación de Servicios de Internet con Seguridad Gestionada, comunicación switch y networking o Proyectos similares en entidades públicas y/o privadas.

Seis (06) Personal Técnico

Dos (02) técnicos con dos (02) años de experiencia como mínimo en actividades de routing y switching

Dos (02) técnicos con dos (02) años de experiencia en actividades con firewalling

Dos (02) técnicos con dos (02) años de experiencia en Administradores de Ancho de Banda

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



MUNICIPALIDAD METROPOLITANA DE LIMA
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

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 contratista 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.*

Firma digital



Firmado digitalmente por
MANTILLA LEON Richard Jean
Paul FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 15:13:44 -05:00

Firma digital



Firmado digitalmente por
HUAYTUA SOLORZANO Flor Du
Liz FAU 20131380951 soft
Motivo: Day V B
Fecha: 15.05.2021 10:29:19 -05:00

Firma digital



Firmado digitalmente por PARRA
WILLIAMS Hubert Emilio FAU
20131380951 soft
Motivo: Day V B
Fecha: 17.05.2021 15:15:01 -05:00