

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

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



**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>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda 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:

- 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.
- 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 marzo, junio y diciembre de 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

BASES INTEGRADAS

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

ADJUDICACIÓN SIMPLIFICADA N°

011-2024-MINSA

PRIMERA CONVOCATORIA

CONTRATACIÓN DE SERVICIO DE

**ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL
MINISTERIO DE SALUD**

Handwritten signatures and marks, including a large stylized signature and a smaller mark below it.

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.

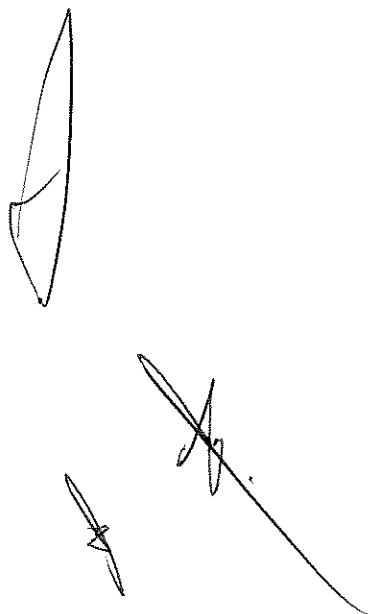
De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión 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)

Handwritten signature and stamp. The signature is a stylized, cursive mark. The stamp is a circular official seal, partially visible and overlapping the signature.

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.mp.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, así como el literal a) del artículo 89 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. Las consultas y observaciones que se formulen sobre el particular, se tienen como no presentadas.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 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. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 del Reglamento.

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). 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.*

1.7. 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

1.8. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el numeral 74.1 y el literal a) del numeral 74.2 del artículo 74 del Reglamento.

En el supuesto de que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se efectúa siguiendo estrictamente el orden establecido en el numeral 91.1 del artículo 91 del Reglamento.

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

Importante

En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP². Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.

1.9. 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.

1.10. 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.

1.11. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

² La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores: www.rnp.gob.pe

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

1.12. OTORGAMIENTO DE LA BUENA PRO

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

1.13. CONSENTIMIENTO DE LA BUENA PRO

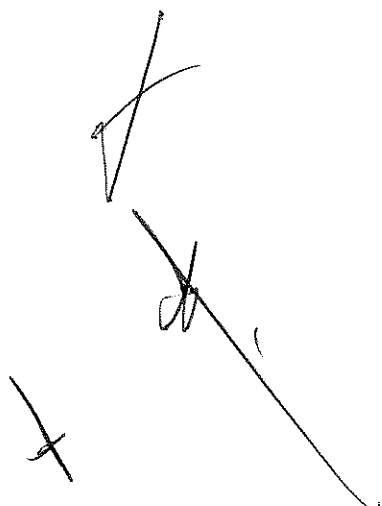
Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

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

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

Importante

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



CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

A través del recurso de apelación se pueden impugnar los actos dictados durante el desarrollo del procedimiento de selección hasta antes del perfeccionamiento del contrato.

El recurso de apelación se presenta ante la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

En los procedimientos de selección según relación de ítems, el valor estimado total del procedimiento determina ante quién se presenta el recurso de apelación.

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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda.
- *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, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.*

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 cinco (5) 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 cinco (5) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de servicios, conforme a lo previsto en la sección específica de las bases.

En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de servicios, cuando el valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de servicios. En caso la Entidad perfeccione el contrato con la recepción de la orden de servicios no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

- En los contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a 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 no superen el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y el numeral 151.2 del artículo 151 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

Importante

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

Advertencia

Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente:

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).
2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.
3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.
4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

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

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

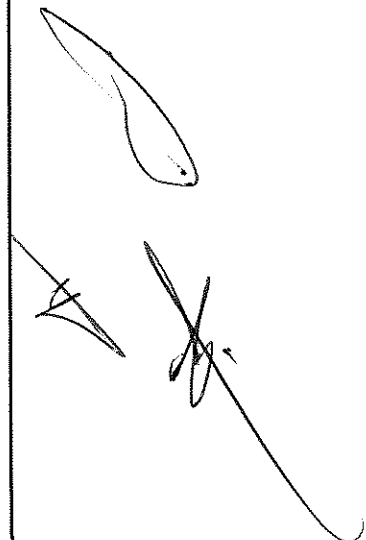
En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

Advertencia

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

3.9. DISPOSICIONES FINALES

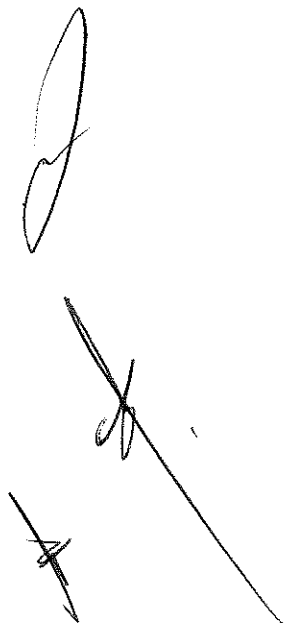
Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

Handwritten signature and stamp in the bottom left corner of the page.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

Handwritten signature and initials in the bottom left corner of the page.

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : MINISTERIO DE SALUD
RUC N° : 20131373237
Domicilio legal : AV. SALAVERRY N°801 – JESÚS MARÍA - LIMA
Teléfono: : 01315-6600 ANEXO 2335
Correo electrónico: : oga044@minsa.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE SALUD

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato 02 N°069-2024-OGA-OA /MINSA el 10 de julio del 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios.

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema A 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 trescientos sesenta

y cinco (365) días calendarios contabilizados a partir del día siguiente de haber suscrito el contrato o de la recepción de la notificación de la orden de servicio, en concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, de manera gratuita, en la Unidad de Adquisiciones y Programación de la Oficina de Abastecimiento, ubicada en el segundo piso del Ministerio de Salud, sito en la Av. Salaverry N°801- Jesús María -Lima.

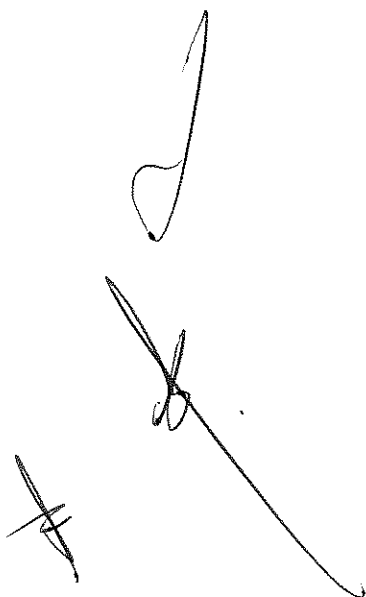
Importante

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

1.10. BASE LEGAL

- Ley N° 31953 Ley de Presupuesto del Sector Público para el Año 2024.
- Ley N° 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Ley N°27815 Ley del Código e Ética de la Función Pública.
- Decreto Supremo N°082-2019-EF, QUE PRUEBA EL Texto Único Ordenado de la Ley N°30225 Ley de Contrataciones del Estado.
- Decreto Supremo N°344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo N°004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N°27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo N°021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley 27806 ley de Transparencia y acceso a la información Pública.
- Resolución N°014-2019-OSCE/PRE, que prueba la Directiva N°002-2019-OSCE/CD "Plan Anual de Contrataciones".
- Resolución Ministerial N°583-2019/MINSA, que aprueba la Directiva Administrativa N°270-MINSA/2019-OGA, "Directiva para la Ejecución de los Procedimientos de Selección de Bienes y/o Servicios para el Ministerio de Salud"

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



CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos³, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- a) Declaración jurada de datos del postor. (Anexo N° 1)
- b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁴ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento (Anexo N°2)
- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3)

³ La omisión del índice no determina la no admisión de la oferta.

⁴ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

- e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**⁵
- 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. Adjuntar obligatoriamente el **Anexo N° 6**.

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los “**Requisitos de Calificación**” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

2.2.2. Documentación de presentación facultativa:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁶.
- b) Solicitud de bonificación por tener la condición de micro y pequeña empresa. **(Anexo N° 11)**

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites “Documentos para la admisión de la oferta”, “Requisitos de calificación” y “Factores de evaluación”.

⁵ En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

⁶ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

2.3. PRESENTACIÓN DEL RECURSO DE APELACIÓN

"El recurso de apelación se presenta ante la Unidad de Trámite Documentario de la Entidad.

En caso el participante o postor opte por presentar recurso de apelación y por otorgar la garantía mediante depósito en cuenta bancaria, se debe realizar el abono en:

N° de Cuenta : 0000-282146
Banco : Banco de la Nación
N° CCI⁷ : 01800000000028214600

2.4. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- d) 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.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁸ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁹. (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado¹⁰.
- j) Estructura de costos¹¹.
- k) Correo para las coordinaciones durante la ejecución contractual, de acuerdo a lo indicado en el numeral 8.3 del Capítulo III de la Sección Específica de las bases.

⁷ En caso de transferencia interbancaria.

⁸ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

⁹ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

¹⁰ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

¹¹ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

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 en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva Participación de Proveedores en Consorcio en las Contrataciones del Estado".
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 y el numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.
- En los contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a 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 no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya¹².
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

2.5. 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 mesa de partes del Ministerio de Salud, ubicada en la Av. Salaverry N°801- Jesús María – Lima, en el horario de 08:00 a 16:30 horas o a través de la mesa de Partes Virtual, con el siguiente link:

https://sgd.minsa.gob.pe/appmesapartesonline/inicio?tid=2*mesadepartes

¹² Según lo previsto en la Opinión N° 009-2016/DTN.

2.6. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en DOCE PAGOS parciales, de acuerdo al siguiente detalle:

Pago	Descripción	Detalle
Primer pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 1er Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura y el 1er Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Segundo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 2do Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.

Pago	Descripción	Detalle
Tercer pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 3er Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Cuarto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 4to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, el 1er Informe de Ingeniería Social solicitado en el numeral 10.3. y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Quinto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 5to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	5% del monto total del contrato.
Sexto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 2do Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura, el 6to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Séptimo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 7mo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, el 2do Informe de Ingeniería Social solicitado en el numeral 10.3. y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Octavo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 8avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.

Pago	Descripción	Detalle
Noveno pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 9no Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Décimo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 10mo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Onceavo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 11avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.
Doceavo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 3er Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura, el 12avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.

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

- Informe del funcionario responsable de la Oficina de Soporte e Infraestructura tecnológica emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Entregable, de acuerdo a lo indicado en el numeral 10 del Capítulo III de la Sección Específica de las bases.

Dicha documentación se debe presentar en mesa de partes del Ministerio de Salud, ubicada en la Av. Salaverry N°801- Jesús María – Lima, en el horario de 08:00 a 16:30 horas o a través de la mesa de Partes Virtual, con el siguiente link:

https://sgd.minsa.gob.pe/appmesapartesonline/inicio?tid=2*mesadepartes

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. TERMINOS DE REFERENCIA

SERVICIO DE ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE SALUD

1. DEPENDENCIA QUE REQUIERE LA CONTRATACIÓN

Oficina de Soporte e Infraestructura Tecnológica - OSIT de la Oficina General de Tecnologías de la Información - OGTI

2. DENOMINACION DE LA CONTRATACIÓN

Servicio de Análisis de Vulnerabilidades sobre los Sistemas de Información del Ministerio de Salud.

3. FINALIDAD PÚBLICA

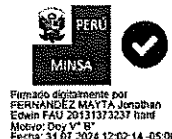
Fortalecer la seguridad de información y seguridad informática del MINISTERIO DE SALUD a través de la implementación de las recomendaciones brindadas en los informes técnicos y el informe ejecutivo que serán presentados en el presente documento.

4. ACTIVIDAD DEL POI RELACIONADA


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
29131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:50:42 -05:00

Categoría presupuestaria	Acciones centrales
Producto / proyecto	Sin producto
Actividad /acción de inversión /obra	Gestión Administrativa
Actividad operativa ID	C0476 – IMPLEMENTAR EL SISTEMA DE INFORMACIÓN DE LA HISTORIA CLÍNICA ELECTRÓNICA – SIHCE DEL MINSA EN ESTABLECIMIENTO DEL PRIMER NIVEL
Nemónico	100

5. DATOS DEL CUADRO MULTIANUAL DE NECESIDADES


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 29131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:02:14 -05:00

Código Del Centro De Costo	11705.08.03
Descripción del centro de costo	OSIT – OFICINA DE SOPORTE E INFRAESTRUCTURA TECNOLÓGICA.
Ítem siga programado	170100040269
Descripción del Ítem	SERVICIO DE ANALISIS DE VULNERABILIDADES

6. OBJETO DE LA CONTRATACIÓN

Contar con un Servicio de Análisis de Vulnerabilidades, para identificar las brechas de seguridad de información y seguridad informática que afectan a los sistemas de información del Ministerio de Salud y que puedan comprometer la confidencialidad, integridad y disponibilidad de la información que forma parte de los sistemas y servicios que se brindan a nivel nacional.

6.1. OBJETIVO ESPECÍFICO

- Contar con los servicios de una persona jurídica que desarrolle el servicio de análisis de vulnerabilidades persistente para los sistemas de información de la organización e infraestructura tecnológica en un periodo de trescientos sesenta y cinco (365) días calendario.

- La solicitud de evaluación de estas aplicaciones será solicitada a demanda, en base al requerimiento de la entidad a través del representante de la Oficina de Soporte e Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información, durante el periodo de ejecución del servicio.
- Identificar, documentar y corregir las vulnerabilidades a las que podría estar expuesta la organización, a través de una bolsa de horas de acompañamiento por parte del proveedor.

7. SISTEMA DE CONTRATACIÓN

SUMA ALZADA

8. DESCRIPCIÓN DEL SERVICIO

8.1. ALCANCE DEL SERVICIO

El presente servicio, debe considerar como parte del alcance del servicio lo detallado en el siguiente cuadro:


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:51:00 -05:00

Nro.	Componente del Alcance	Periodicidad
1	Ethical Hacking a nivel de infraestructura	03 evaluaciones por año.
2	Ethical Hacking de aplicaciones a demanda	100 aplicaciones, durante todo el periodo contractual ¹ .
3	Pruebas de Ingeniería Social	02 phishing en el año. 02 revisiones de escritorios limpios al año.
4	Ejercicios de Cibervigilancia con periodicidad mensual	Continuo.


Firmado digitalmente por
FERNANDEZ MAYTA, Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:02:39 -05:00


- Las pruebas se realizarán desde las siguientes perspectivas: CAJA NEGRA y CAJA GRIS.
- El MINSA brindará la relación de aplicaciones web y/o sistemas de información y/o web services y los datos relacionado a las bases de datos, sobre las cuales se ejecutará el servicio, la misma que se brindará a través de correo electrónico el cual será remitido por personal responsable del servicio de parte de la Oficina de Soporte e Infraestructura Tecnológica.
- Para la realización de las pruebas en CAJA GRIS se brindarán credenciales de acceso al sistema de información, como mínimo dos (02) perfiles de acceso.
- Para el componente Ethical Hacking de aplicaciones a demanda, se considera que:
 - Cada evaluación a demanda será sobre una aplicación nueva, solo en casos excepcionales se realizará una evaluación sobre la misma aplicación.
 - Entre las aplicaciones a evaluar, se tiene un máximo de 25 módulos; asimismo, de requerirse los manuales de usuarios serán brindados al iniciar la evaluación de cada aplicación².


8.2. ESPECIFICACIONES DEL SERVICIO.

- La ejecución del servicio no debe causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red de la institución.

¹ De acuerdo a la absolución de la consulta N° 1 del participante JACKSECURITY.COM SAC.
² De acuerdo a la absolución de la consulta N° 1 del participante JACKSECURITY.COM SAC.

- El Contratista, en coordinación con el personal técnico del MINSA, elaborarán los cronogramas para la ejecución de la evaluación de seguridad y pruebas de Ethical Hacking al inicio del servicio.
- Se deberá firmar un acuerdo de CONFIDENCIALIDAD entre el Contratista y MINSA, en el cual se estipulará la prohibición de la difusión de las pruebas realizadas, el resultado de las mismas o de la información brindada por parte de la institución, las cuales no hayan sido autorizadas.
- Bajo ninguna circunstancia y en ningún momento se generará algún tipo de cambio sobre los sistemas y/o información a las que se logre acceso.
- El Contratista deberá indicar las herramientas, equipos y/o productos que utilizará durante la ejecución de la evaluación de seguridad y pruebas de penetración. En caso se utilicen herramientas gratuitas, **el Contratista las pondrá a disposición de la institución**; el uso de herramientas gratuitas debe garantizar el mismo nivel de análisis que las herramientas de análisis licenciadas o de pago; el objetivo principal es tener un diagnóstico y análisis completo.
- La metodología utilizada para la ejecución del Ethical Hacking, debe estar basada en los manuales de seguridad OSSTMM (Open Source Security Testing Methodology Manual) y OWASP Testing Guide v4.0.
- Las vulnerabilidades identificadas durante la evaluación y Ethical Hacking deben disponer de trazabilidad, a fin de que el MINSA disponga de las evidencias respectivas.
- Las recomendaciones emitidas para el MINSA, deben ser aplicables para que puedan ser implementadas por la organización.
- Los informes y recomendaciones entregados al MINSA, deben encontrarse en ESPAÑOL, a excepción de los reportes que puedan ser emitidos directamente por las herramientas utilizadas, los cuales servirán como anexos a los informes presentados.
- Todos los entregables serán presentados en medio óptico (01 CD-ROM o DVD) y cifrados con una contraseña debido a la confidencialidad de la información.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
ID: 131373237 hard
Motivo: Doc V° B°
Fecha: 31.07.2024 11:51:10 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doc V° B°
Fecha: 31.07.2024 12:02:46 -05:00

8.3. COMPONENTES DEL SERVICIO

Realizar el análisis de vulnerabilidades de las aplicaciones detalladas en el alcance del servicio en un periodo de trescientos sesenta y cinco (365) días calendario. La solicitud de evaluación será realizada a demanda, la misma que la podrá realizar mediante correo electrónico remitido por personal de la Oficina de Soporte e Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información, con una anticipación de un (01) día previo al inicio del análisis.

El servicio podrá brindarse de manera remota desde las instalaciones del proveedor. En caso de requerir asistir presencialmente a las instalaciones de la entidad, se realizarán las coordinaciones correspondientes del caso.

El proveedor deberá indicar el correo para las coordinaciones durante la ejecución contractual del servicio, dicha información debe ser presentada para la suscripción del contrato.

A. COMPONENTE ETHICAL HACKING

PRUEBAS DE PENETRACIÓN EXTERNA (CAJA NEGRA)

En estas pruebas se emplea la información pública disponible de la organización, o se evalúa como usuario anónimo o mínimo privilegio. Esto se puede utilizar para evaluar los mecanismos perimetrales de seguridad de la organización.

PRUEBAS DE PENETRACIÓN INTERNO (CAJA GRIS)

Se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización. En este tipo de pruebas se utiliza la información privada, otorgada por Caja, se evalúa como usuarios usando distintos roles y niveles de acceso a los sistemas.

En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada o de usuarios con privilegios de acceso.

Nro.	Prueba	Cantidad
1	Cantidad de direcciones IP públicas (expuestas a Internet)	250
3	Cantidad aproximada de direcciones IP de servidores internos	500
4	Cantidad aproximada de direcciones IP de estaciones de trabajo	500

La metodología de Ethical Hacking aplicado por el contratista para la verificación de la seguridad de la infraestructura, se centrará en la evaluación de controles de autenticación, configuración segura y aplicación de parches a nivel del sistema operativo, servicios de red y base de datos.

Como producto del servicio, se obtendrán las vulnerabilidades de la Infraestructura clasificadas según su nivel de riesgo, las cuales estarán acompañadas con procedimientos o recomendaciones para su mitigación.

Culminado el proyecto, el proveedor deberá emitir un informe de las vulnerabilidades resueltas por la organización.

SE DEBERÁN CUMPLIR CON LAS SIGUIENTES ETAPAS:

RECONOCIMIENTO DE OBJETIVOS:

- Obtención de información DNS, ubicaciones, personas de contacto, Whois, Google y otros sitios relevantes para la obtención de información.
- Búsquedas de URLs internas u ocultas de los sistemas a evaluar y extracción de información.

EXPLORACIÓN:

- Exploración de protocolos que se ejecutan sobre IP.
- Exploración de puertos: syn scan, ack scan, UDP scan, xmas scan, fin scan, null scan, RPC scan, idle scan.
- Identificación de servicios y obtención de banners.
- Identificación de sistemas operativos utilizando técnicas activas de estímulo/respuesta.

IDENTIFICACIÓN DE VULNERABILIDADES A NIVEL DE SISTEMAS OPERATIVOS:

- Enumeración de recursos de sistemas operativos UNIX/Linux con showmount y rpcinfo.
- Enumeración de recursos de sistemas operativos Windows mediante sesiones nulas.
- Enumeración de servicios SNMP.
- Verificación de configuraciones inseguras


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hsgd
Motivo: Doy V° B°
Fecha: 31.07.2024 11:51:19 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:02:55 -05:00

- Identificación de parches no aplicados.

IDENTIFICACIÓN DE VULNERABILIDADES A NIVEL DE SERVICIOS:

- Identificación de servicios mediante captura de banners.
- Identificación de servicios mediante huellas digitales.
- Identificación de servidores HTTP.
- Verificación de configuraciones inseguras.
- Identificación de parches no aplicados.
- Verificación de Vulnerabilidades.
- Verificación de vulnerabilidades mediante la explotación de las mismas utilizando herramientas propietarias y de fuente de libre disponibilidad como Metasploit Framework, Exploit-DB e Injector, o algún otro.

OBTENCIÓN DE ACCESO:

- Obtención de acceso Shell al servidor mediante la explotación de vulnerabilidades.
- Creación de cuentas de usuario en el sistema operativo o servicio atacado.

B. COMPONENTE DE ETHICAL HACKING DE APLICACIONES A DEMANDA

REVISIÓN DE APLICACIONES (CAJA NEGRA O CAJA GRIS)

Como parte de las pruebas de penetración consideradas deben incluirse la revisión de aplicaciones que el representante de la Oficina de Soporte e Infraestructura Tecnológica remitirá mediante correo electrónico, la misma que debe ejecutarse en un plazo máximo de treinta (30) días calendario, contabilizados a partir del día siguiente de remitida la solicitud de evaluación³.

La metodología de Ethical Hacking aplicada por el contratista para la verificación de seguridad de Aplicaciones, se centrará en la evaluación de controles utilizados para la autenticación, manejo de sesiones y validación de datos de entrada. Asimismo, se identificarán problemas de configuración, transmisión insegura de datos y divulgación de información sensible.

Como producto de la evaluación se obtienen las vulnerabilidades de la Aplicación Web clasificadas según el nivel de riesgo, las cuales son acompañadas con recomendaciones aplicables a su mitigación.

Los controles que serán evaluados se encuentran alineados al OWASP - Web Security Testing Guide (WSTG) en su versión v4.2.

Recopilación de información	Nombre de la prueba	Objetivos
WSTG-INFO-01	Llevar a cabo un reconocimiento de descubrimiento de motores de búsqueda para detectar fugas de información	- Identificar qué información confidencial de diseño y configuración de la aplicación, el sistema o la organización está expuesta directamente (en el sitio web de la organización) o


³ De acuerdo a la absolución de la consulta N° 1 del participante JACKSECURITY.COM SAC.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131573237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:51:36 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:03:19 -05:00

Recopilación de información	Nombre de la prueba	Objetivos
		indirectamente (a través de servicios de terceros).
WSTG-INFO-02	Servidor web de huellas dactilares	- Determinar la versión y el tipo de un servidor web en ejecución para permitir un mayor descubrimiento de cualquier vulnerabilidad conocida.
WSTG-INFO-03	Revise los metarchivos del servidor web para detectar fugas de información	- Identificar rutas y funcionalidades ocultas u ofuscadas a través del análisis de archivos de metadatos. - Extraer y mapear otra información que podría conducir a una mejor comprensión de los sistemas en cuestión.
WSTG-INFO-04	Enumerar aplicaciones en el servidor web	- Enumerar las aplicaciones dentro del alcance que existen en un servidor web.
WSTG-INFO-05	Revisar el contenido de la página web para detectar fugas de información	- Revisar los comentarios y metadatos de la página web para encontrar cualquier fuga de información. - Reúna archivos JavaScript y revise el código JS para comprender mejor la aplicación y encontrar cualquier fuga de información. - Identifique si existen archivos de mapas de origen u otros archivos de depuración front-end.
WSTG-INFO-06	Identificar los puntos de entrada de la aplicación	- Identificar posibles puntos de entrada e inyección a través del análisis de solicitudes y respuestas.
WSTG-INFO-07	Asignar rutas de ejecución a través de la aplicación	- Asignar la aplicación de destino y comprender los principales flujos de trabajo.
WSTG-INFO-08	Marco de aplicaciones web de huellas dactilares	- Huella digital de los componentes que utilizan las aplicaciones web.
WSTG-INFO-09	Aplicación web de huellas dactilares	
WSTG-INFO-10	Arquitectura de aplicaciones de mapas	- Generar un mapa de la aplicación en cuestión en base a la investigación realizada.

Pruebas de gestión de configuración e implementación	Nombre de la prueba	Objetivos
WSTG-CONF-01	Configuración de la infraestructura de red de prueba	- Revisar las configuraciones de las aplicaciones establecidas en la red y validar que no sean vulnerables. - Validar que los marcos y sistemas utilizados sean seguros y no susceptibles a vulnerabilidades conocidas debido a software sin


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:51:47 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:03:28 -05:00

Pruebas de gestión de configuración e implementación	Nombre de la prueba	Objetivos
		mantenimiento o configuraciones y credenciales predeterminadas.
WSTG-CONF-02	Configuración de la plataforma de aplicaciones de prueba	- Asegúrese de que se hayan eliminado los archivos predeterminados y conocidos. - Validar que no quede código de depuración ni extensiones en los entornos de producción. - Revisar los mecanismos de registro establecidos para la aplicación.
WSTG-CONF-03	Manejo de extensiones de archivo de prueba para información confidencial	- Dirbust extensiones de archivos confidenciales o extensiones que pueden contener datos sin procesar (*por ejemplo, * secuencias de comandos, datos sin procesar, credenciales, etc.). - Valide que no existan omisiones del marco del sistema en el conjunto de reglas.
WSTG-CONF-04	Revise la copia de seguridad antigua y los archivos sin referencia en busca de información confidencial	- Busque y analice archivos sin referencia que puedan contener información confidencial.
WSTG-CONF-05	Enumerar interfaces de administración de aplicaciones e infraestructura	- Identificar interfaces y funciones de administrador ocultas.
WSTG-CONF-06	Probar métodos HTTP	- Enumerar los métodos HTTP admitidos. - Prueba de bypass de control de acceso. - Probar vulnerabilidades XST. - Pruebe las técnicas de anulación del método HTTP.
WSTG-CONF-07	Probar la seguridad de transporte estricta de HTTP	- Revisar la cabecera del HSTS y su vigencia.
WSTG-CONF-08	Probar la política de dominios cruzados de RIA	- Revisar y validar los archivos de políticas.
WSTG-CONF-09	Permiso de archivo de prueba	- Revise e identifique los permisos de archivos no autorizados.
WSTG-CONF-10	Prueba de adquisición de subdominio	- Enumerar todos los dominios posibles (anteriores y actuales). - Identificar dominios olvidados o mal configurados.
WSTG-CONF-11	Prueba de almacenamiento en la nube	- Evaluar que la configuración de control de acceso a los servicios de almacenamiento esté correctamente implementada.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 11:51:55 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 12:03:36 -05:00

Pruebas de gestión de identidad	Nombre de la prueba	Objetivos
WSTG-IDNT-01	Definiciones de roles de prueba	- Identificar y documentar los roles utilizados por la aplicación. - Intentar cambiar, cambiar o acceder a otro rol. - Revisar la granularidad de los roles y las necesidades detrás de los permisos otorgados.
WSTG-IDNT-02	Proceso de registro de usuario de prueba	- Verificar que los requisitos de identidad para el registro de usuarios estén alineados con los requisitos comerciales y de seguridad. - Validar el proceso de registro.
WSTG-IDNT-03	Proceso de aprovisionamiento de cuenta de prueba	- Verificar qué cuentas pueden provisionar otras cuentas y de qué tipo.
WSTG-IDNT-04	Pruebas de enumeración de cuenta y cuenta de usuario adivinable	- Revisar los procesos relacionados con la identificación del usuario (*ej.* registro, inicio de sesión, etc.). - Enumerar a los usuarios cuando sea posible a través del análisis de respuestas.
WSTG-IDNT-05	Prueba de política de nombre de usuario débil o no aplicada	- Determinar si una estructura de nombre de cuenta coherente hace que la aplicación sea vulnerable a la enumeración de cuentas. - Determinar si los mensajes de error de la aplicación permiten la enumeración de cuentas.

Pruebas de autenticación	Nombre de la prueba	Objetivos
WSTG-ATHN-01	Prueba de credenciales transportadas a través de un canal cifrado	- Evaluar si algún caso de uso del sitio web o aplicación hace que el servidor o el cliente intercambien credenciales sin cifrar.
WSTG-ATHN-02	Prueba de credenciales predeterminadas	- Enumerar las solicitudes de credenciales por defecto y validar si aún existen. - Revisar y evaluar nuevas cuentas de usuario y si se crean con valores predeterminados o patrones identificables.
WSTG-ATHN-03	Prueba de mecanismo de bloqueo débil	- Evaluar la capacidad del mecanismo de bloqueo de cuentas para mitigar la adivinación de contraseñas por fuerza bruta. - Evaluar la resistencia del mecanismo de desbloqueo al desbloqueo no autorizado de cuentas.
WSTG-ATHN-04	Prueba para eludir el esquema de autenticación	- Asegúrese de que la autenticación se aplique en todos los servicios que la requieran.


Firmado digitalmente por CHALCO
MALDORADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:52:08 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:03:53 -05:00

Pruebas de autenticación	Nombre de la prueba	Objetivos
WSTG-ATHN-05	Prueba para recordar contraseña vulnerable	- Validar que la sesión generada se gestione de forma segura y no poner en peligro las credenciales del usuario.
WSTG-ATHN-06	Prueba de debilidades de caché del navegador	- Revisar si la aplicación almacena información confidencial en el lado del cliente. - Revisar si el acceso puede ocurrir sin autorización.
WSTG-ATHN-07	Prueba de política de contraseña débil	- Determinar la resistencia de la aplicación frente a la adivinación de contraseñas por fuerza bruta utilizando los diccionarios de contraseñas disponibles mediante la evaluación de los requisitos de longitud, complejidad, reutilización y antigüedad de las contraseñas.
WSTG-ATHN-08	Prueba de respuesta de pregunta de seguridad débil	- Determinar la complejidad y la sencillez de las preguntas. - Evaluar las posibles respuestas de los usuarios y las capacidades de fuerza bruta.
WSTG-ATHN-09	Prueba de funcionalidades de cambio o restablecimiento de contraseña débil	- Determinar la resistencia de la aplicación a la subversión del proceso de cambio de cuenta permitiendo que alguien cambie la contraseña de una cuenta. - Determinar la resistencia de la funcionalidad de restablecimiento de contraseñas contra adivinar o pasar por alto.
WSTG-ATHN-10	Prueba de autenticación más débil en canal alternativo	- Identificar canales de autenticación alternativos. - Evaluar las medidas de seguridad utilizadas y si existen desvíos en los canales alternativos.

Pruebas de autorización	Nombre de la prueba	Objetivos
WSTG-ATHZ-01	Prueba de inclusión de archivos transversales de directorios	- Identificar los puntos de inyección que pertenecen al recorrido de la ruta. - Evaluar las técnicas de elusión e identificar el alcance del recorrido de la ruta.
WSTG-ATHZ-02	Pruebas para eludir el esquema de autorización	- Evaluar si es posible el acceso horizontal o vertical.
WSTG-ATHZ-03	Pruebas de escalada de privilegios	- Identificar puntos de inyección relacionados con la manipulación de privilegios. - Fuzz o intentar eludir las medidas de seguridad.
WSTG-ATHZ-04	Pruebas de referencias de objetos directos inseguros	- Identificar puntos donde pueden ocurrir referencias a objetos. - Evaluar las medidas de control de acceso y si son vulnerables a IDOR.


Firmado digitalmente por CHALCO
ALDONADO Jose Luis FAU
ID:131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:52:17 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Covier FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:04:02 -05:00


Pruebas de gestión de sesiones	Nombre de la prueba	Objetivos
WSTG-SESS-01	Prueba del esquema de gestión de sesiones	- Reúna tokens de sesión, para el mismo usuario y para diferentes usuarios cuando sea posible. - Analice y asegúrese de que exista suficiente aleatoriedad para detener los ataques de falsificación de sesión. - Modificar cookies que no estén firmadas y contengan información manipulable.
WSTG-SESS-02	Prueba de atributos de cookies	- Asegurarse de que se ha establecido la configuración de seguridad adecuada para las cookies.
WSTG-SESS-03	Prueba de Fijación de Sesión	- Analizar el mecanismo de autenticación y su flujo. - Forzar cookies y evaluar el impacto.
WSTG-SESS-04	Prueba de variables de sesión expuestas	- Asegúrese de que se implemente el cifrado adecuado. - Revisar la configuración de almacenamiento en caché. - Evaluar la seguridad de los canales y métodos.
WSTG-SESS-05	Pruebas de falsificación de solicitudes entre sitios	- Determinar si es posible iniciar solicitudes en nombre de un usuario que no sean iniciadas por el usuario.
WSTG-SESS-06	Prueba de funcionalidad de cierre de sesión	- Evaluar la interfaz de usuario de cierre de sesión. - Analice el tiempo de espera de la sesión y si la sesión se cancela correctamente después del cierre de sesión.
WSTG-SESS-07	Tiempo de espera de la sesión de prueba	- Validar que existe un tiempo de espera de sesión difícil.
WSTG-SESS-08	Prueba de desconcierto de sesión	- Identificar todas las variables de sesión. - Rompe el flujo lógico de generación de sesiones.
WSTG-SESS-09	Prueba de secuestro de sesión	- Identificar cookies de sesión vulnerables. - Secuestrar cookies vulnerables y evaluar el nivel de riesgo.

Pruebas de validación de datos	Nombre de la prueba	Objetivos
WSTG-INPV-01	Pruebas de secuencias de comandos reflejadas entre sitios	- Identificar variables que se reflejan en las respuestas. - Evaluar la entrada que aceptan y la codificación que se aplica a la devolución (si corresponde).
WSTG-INPV-02	Pruebas de secuencias de comandos entre sitios almacenadas	- Identificar la entrada almacenada que se refleja en el lado del cliente. - Evaluar la entrada que aceptan y la codificación


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Dey "Y" 8°
Fecha: 31.07.2024 11:52:25 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Dey "Y" 8°
Fecha: 31.07.2024 12:04:09 -05:00

Pruebas de validación de datos	Nombre de la prueba	Objetivos
		que se aplica a la devolución (si corresponde).
WSTG-INPV-03	Prueba de manipulación de verbos HTTP	
WSTG-INPV-04	Pruebas de contaminación de parámetros HTTP	- Identificar el backend y el método de análisis utilizado. - Evalúe los puntos de inyección e intente omitir los filtros de entrada mediante HPP.
WSTG-INPV-05	Pruebas de inyección SQL	- Identificar puntos de inyección SQL. - Evaluar la severidad de la inyección y el nivel de acceso que se puede lograr a través de ella.
WSTG-INPV-06	Prueba de inyección LDAP	- Identificar puntos de inyección LDAP. - Evaluar la severidad de la inyección.
WSTG-INPV-07	Pruebas de inyección XML	- Identificar puntos de inyección de XML. - Evaluar los tipos de exploits que se pueden lograr y su gravedad.
WSTG-INPV-08	Pruebas de inyección de SSI	- Identificar los puntos de inyección de SSI. - Evaluar la severidad de la inyección.
WSTG-INPV-09	Prueba de inyección XPath	- Identificar los puntos de inyección de XPATH.
WSTG-INPV-10	Pruebas de inyección IMAP SMTP	- Identificar puntos de inyección IMAP/SMTP. - Comprender el flujo de datos y la estructura de despliegue del sistema. - Evaluar los impactos de la inyección.
WSTG-INPV-11	Pruebas de inyección de código	- Identificar puntos de inyección donde se puede inyectar código en la aplicación. - Evaluar la severidad de la inyección.
WSTG-INPV-12	Prueba de inyección de comandos	- Identificar y evaluar los puntos de inyección de mando.
WSTG-INPV-13	Prueba de inyección de cadenas de formato	- Evaluar si inyectar especificadores de conversión de cadena de formato en campos controlados por el usuario provoca un comportamiento no deseado de la aplicación.
WSTG-INPV-14	Pruebas de vulnerabilidad incubada	- Identificar las inyecciones que están almacenadas y requieren un paso de retiro de la inyección almacenada. - Comprender cómo podría ocurrir un paso de recuperación. - Configure los oyentes o active el paso de recuperación si es posible.
WSTG-INPV-15	Pruebas de contrabando de división HTTP	- Evaluar si la aplicación es vulnerable a splitting, identificando qué posibles


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20191373237 hard
Módulo: Doy V° B°
Fecha: 31.07.2024 11:52:34 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131375237 hard
Módulo: Doy V° B°
Fecha: 31.07.2024 12:04:18 -05:00


Pruebas de validación de datos	Nombre de la prueba	Objetivos
		ataques son realizables. - Evaluar si la cadena de comunicación es vulnerable al contrabando, identificando qué posibles ataques son realizables.
WSTG-INPV-16	Prueba de solicitudes entrantes HTTP	- Supervise todas las solicitudes HTTP entrantes y salientes al servidor web para inspeccionar cualquier solicitud sospechosa. - Supervise el tráfico HTTP sin cambios en el proxy del navegador del usuario final o en la aplicación del lado del cliente.
WSTG-INPV-17	Prueba de inyección de encabezado de host	- Evaluar si el encabezado del host se analiza dinámicamente en la aplicación. - Eludir los controles de seguridad que se basan en el encabezado.
WSTG-INPV-18	Prueba de inyección de plantilla del lado del servidor	- Detectar puntos de vulnerabilidad de inyección de plantilla. - Identificar el motor de plantillas. - Construir el exploit.
WSTG-INPV-19	Pruebas de falsificación de solicitudes del lado del servidor	- Identificar los puntos de inyección de SSRF. - Probar si los puntos de inyección son explotables. - Evaluar la gravedad de la vulnerabilidad.

Manejo de errores	Nombre de la prueba	Objetivos
WSTG-ERRH-01	Pruebas para el manejo inadecuado de errores	- Identificar la salida de error existente. - Analizar los diferentes resultados devueltos.
WSTG-ERRH-02	Prueba de rastros de pila	

Criptografía	Nombre de la prueba	Objetivos
WSTG-CRYP-01	Pruebas de seguridad de capa de transporte débil	- Validar la configuración del servicio. - Revisar la fuerza criptográfica y la validez del certificado digital. - Asegúrese de que la seguridad TLS no se pueda eludir y se implemente correctamente en toda la aplicación.
WSTG-CRYP-02	Pruebas para Padding Oracle	- Identifique los mensajes cifrados que se basan en el relleno. - Intente romper el relleno de los mensajes cifrados y analice los mensajes de error devueltos para un análisis más detallado.
WSTG-CRYP-03	Pruebas de información confidencial enviada a través de canales no cifrados	- Identificar la información sensible transmitida a través de los distintos canales. - Evaluar la privacidad y seguridad de los canales utilizados.


Criptografía	Nombre de la prueba	Objetivos
WSTG-CRYP-04	Pruebas de cifrado débil	- Proporcionar una guía para la identificación de usos e implementaciones de encriptación débil o hashing.

Pruebas de lógica de negocios	Nombre de la prueba	Objetivos
WSTG-BUSL-01	Prueba de validación de datos de lógica empresarial	- Identificar puntos de inyección de datos. - Valide que todas las comprobaciones se realicen en el back-end y no se puedan omitir. - Intentar romper el formato de los datos esperados y analizar cómo los maneja la aplicación.
WSTG-BUSL-02	Capacidad de prueba para falsificar solicitudes	- Revise la documentación del proyecto en busca de funcionalidades adivinables, predecibles u ocultas de los campos. - Inserte datos lógicamente válidos para evitar el flujo de trabajo de lógica comercial normal.
WSTG-BUSL-03	Comprobaciones de integridad de la prueba	- Revisar la documentación del proyecto para los componentes del sistema que mueven, almacenan o manejan datos. - Determinar qué tipo de datos es lógicamente aceptable por el componente y contra qué tipos debe protegerse el sistema. - Determinar a quién se le debe permitir modificar o leer esos datos en cada componente. - Intente insertar, actualizar o eliminar valores de datos utilizados por cada componente que no deberían permitirse según el flujo de trabajo de la lógica empresarial.
WSTG-BUSL-04	Prueba de temporización del proceso	- Revisar la documentación del proyecto para conocer la funcionalidad del sistema que puede verse afectada por el tiempo. - Desarrollar y ejecutar casos de mal uso.
WSTG-BUSL-05	Prueba Número de veces que se puede usar una función Límites	- Identificar las funciones que deben poner límites a los tiempos en que pueden ser llamadas. - Evaluar si existe un límite lógico establecido en las funciones y si está debidamente validado.
WSTG-BUSL-06	Pruebas de elusión de flujos de trabajo	- Revise la documentación del proyecto en busca de métodos para omitir o realizar pasos en el proceso de solicitud en un orden diferente del flujo de lógica


Firmado digitalmente por CHALCO MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:52:42 -05:00


Firmado digitalmente por FERNANDEZ MAYTA Jonathan Edwen FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:04:26 -05:00


Firmado digitalmente por CHALCO MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Day V" B"
Fecha: 31.07.2024 11:52:51 -05:00


Firmado digitalmente por FERNANDEZ MAYTA Jonathan Edwin FAU 20131373237 hard
Motivo: Day V" B"
Fecha: 31.07.2024 12:04:34 -05:00

Pruebas de lógica de negocios	Nombre de la prueba	Objetivos
		de negocios previsto. - Desarrolle un caso de uso indebido e intente eludir todos los flujos lógicos identificados.
WSTG-BUSL-07	Pruebe las defensas contra el mal uso de la aplicación	- Generar notas de todas las pruebas realizadas contra el sistema. - Revisar qué pruebas tenían una funcionalidad diferente según la entrada agresiva. - Comprender las defensas existentes y verificar si son suficientes para proteger el sistema contra técnicas de derivación.
WSTG-BUSL-08	Carga de prueba de tipos de archivos inesperados	- Revisar la documentación del proyecto para los tipos de archivos que son rechazados por el sistema. - Verifique que los tipos de archivos no deseados sean rechazados y manejados de manera segura. - Verifique que las cargas por lotes de archivos sean seguras y no permitan eludir las medidas de seguridad establecidas.
WSTG-BUSL-09	Carga de prueba de archivos maliciosos	- Identificar la funcionalidad de carga de archivos. - Revisar la documentación del proyecto para identificar qué tipos de archivos se consideran aceptables y qué tipos se considerarían peligrosos o maliciosos. - Determinar cómo se procesan los archivos cargados. - Obtener o crear un conjunto de archivos maliciosos para realizar pruebas. - Intente cargar los archivos maliciosos en la aplicación y determine si se aceptan y procesan.

Pruebas del lado del cliente	Nombre de la prueba	Objetivos
WSTG-CLNT-01	Pruebas para Cross Site Scripting basado en DOM	- Identificar sumideros DOM. - Cree cargas útiles que pertenezcan a cada tipo de sumidero.
WSTG-CLNT-02	Prueba de ejecución de JavaScript	- Identificar sumideros y posibles puntos de inyección de JavaScript.
WSTG-CLNT-03	Prueba de inyección de HTML	- Identificar puntos de inyección de HTML y evaluar la gravedad del contenido inyectado.
WSTG-CLNT-04	Prueba de redirección de URL del lado del cliente	- Identificar puntos de inyección que manejan URLs o rutas. - Evaluar las ubicaciones a las que el sistema podría redirigir.

 
Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 11:53:01 -05:00

 
Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 12:04:43 -05:00

Pruebas del lado del cliente	Nombre de la prueba	Objetivos
WSTG-CLNT-05	Pruebas de inyección de CSS	- Identificar puntos de inyección de CSS. - Evaluar el impacto de la inyección.
WSTG-CLNT-06	Pruebas de manipulación de recursos del lado del cliente	- Identificar sumideros con validación de entrada débil. - Evaluar el impacto de la manipulación de recursos.
WSTG-CLNT-07	Probar el intercambio de recursos de origen cruzado	- Identificar puntos finales que implementan CORS. - Asegúrese de que la configuración de CORS sea segura o inofensiva.
WSTG-CLNT-08	Prueba de intermitencia entre sitios	- Descompilar y analizar el código de la aplicación. - Evaluar entradas de sumideros y usos de métodos inseguros.
WSTG-CLNT-09	Pruebas de secuestro de clics	- Comprender las medidas de seguridad vigentes. - Evaluar qué tan estrictas son las medidas de seguridad y si son evitables.
WSTG-CLNT-10	Prueba de WebSockets	- Identificar el uso de WebSockets. - Evaluar su implementación utilizando las mismas pruebas en canales HTTP normales.
WSTG-CLNT-11	Prueba de mensajería web	- Evaluar la seguridad del origen del mensaje. - Valide que esté usando métodos seguros y validando su entrada.
WSTG-CLNT-12	Probar el almacenamiento del navegador	- Determinar si el sitio web almacena datos confidenciales en el almacenamiento del lado del cliente. - El manejo del código de los objetos de almacenamiento debe examinarse en busca de posibilidades de ataques de inyección, como el uso de entradas no validadas o bibliotecas vulnerables.
WSTG-CLNT-13	Pruebas para la inclusión de secuencias de comandos en sitios cruzados	- Localizar datos confidenciales en todo el sistema. - Evaluar la fuga de datos sensibles a través de diversas técnicas.

Pruebas de API	Nombre de la prueba	Objetivos
WSTG-APIT-01	Probando GraphQL	- Evaluar que se implemente una configuración segura y lista para producción. - Validar todos los campos de entrada contra ataques genéricos. - Asegurarse de que se aplican los controles de acceso adecuados.

C. COMPONENTE DE INGENIERÍA SOCIAL

CONSIDERAR 02 EJERCICIOS DE INGENIERÍA SOCIAL AL AÑO: Los escenarios serán

definidos durante el transcurso del proyecto. Se consideran dentro del ejercicio las siguientes pruebas.

Nro.	PRUEBAS A REALIZAR	CANTIDAD
1	Pruebas de phishing	2 veces al año (500 personas)
2	Pruebas de Revisión de Escritorios limpios	2 veces al año

Las pruebas deberán ser coordinadas durante el transcurso del proyecto.

D. COMPONENTE DE CIBERVIGILANCIA

EJERCICIOS DE CIBERVIGILANCIA

Durante el desarrollo del proyecto se deberán desarrollar las siguientes actividades asociadas a actividades de ciberseguridad:

Nro.	Actividad a Realizar	Periodicidad
1	Monitoreo de Redes Sociales y Exposición en Internet	Mensual
2	Detección y monitoreo de ataques de PHISHING	Mensual
3	Alerta de nuevas vulnerabilidades y riesgos de seguridad	Mensual y a demanda


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:53:11 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:04:53 -05:00

MONITOREO DE REDES SOCIALES Y EXPOSICIÓN EN INTERNET

A través de técnicas OSINT (Open Source Intelligence) se realizan búsquedas estructuradas de información expuesta de la organización en Internet. Las técnicas de búsqueda de información incluyen:

- Análisis de búsqueda de información en buscadores: Google y Bing.
- Análisis de búsqueda de información en buscadores de dispositivos: SHODAN, ZoomEye. Esto con la finalidad de encontrar algún vector de ciberataque.
- Identificación de correos electrónicos expuestos a Internet.
- Búsqueda de suplantación de identidad en redes sociales (perfiles falsos): Facebook, Twitter, Instagram y LinkedIn.
- Búsqueda de exposición de información en portales del tipo GITHUB, PASTEBIN.
- Búsqueda de vulnerabilidad expuestas a Internet y anexada por buscadores.
- Monitoreo y búsqueda de información en la Deep/Dark Web, como campañas de fraude específicas, campañas de malware dirigido a la empresa.
- Inteligencia y protección contra el fraude asociado con el uso ilegítimo de la marca de la empresa.
- Monitoreo de los aplicativos falsos en los portales oficiales y no oficiales de software para móviles.
- Actividades de hacktivismo, búsqueda de activos incluidos en la lista negra.
- Detección de información corporativa de acceso restringido fuera del entorno de TI de la empresa como tarjetas de crédito, usuarios y credenciales, documentos sensibles, etc.

DETECCIÓN Y MONITOREO DE ATAQUES DE PHISHING

A través del monitoreo y alerta de servidores DNS se realizan búsquedas con el objetivo de identificar dominios y sub-dominios que mantengan un grado de similitud con el de la organización.

El objetivo es identificar de manera oportuna dominios que pueden ser utilizados por atacantes informáticos para realizar ataques de Ingeniería Social. Las actividades asociadas son:

- Consultas recurrentes de a servidores DNS.
- Análisis de cabeceras de protocolo SMTP (correo electrónico) en caso de recibir algún ataque de PHISHING.
- Alerta al proveedor de dominio y/o hosting para contener el ataque en el menor tiempo posible (Identificación de suplantación de dominio).
- Alerta a los buscadores en Internet para emisión de alertas de ataque en navegadores.
- El Contratista realizará el proceso de TAKE DOWN (dar de baja) al portal de donde se realiza el ataque informático. Es importante mencionar que este proceso depende las políticas de seguridad de terceros (Hosting, Facebook, Twitter, etc) por lo que el tiempo de realización es variante.

ALERTA DE NUEVAS VULNERABILIDADES Y RIESGOS DE SEGURIDAD

El servicio de cibervigilancia incluye un proceso de **ALERTA CONTINUA Y TEMPRANA** ante la aparición de nuevas vulnerabilidades que puedan afectar la infraestructura tecnológica y sistemas de información de la organización.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 11:53:20 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131375237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 12:05:00 -05:00

Se tiene contabilizado que el año se identifican **más de 15 mil vulnerabilidades** según reportes de CVEDETAILS (<https://www.cvedetails.com/browse-bydate.php>) por lo que el conocimiento e identificación de las mismas, de manera temprana, pueden disminuir el RIESGO e IMPACTO en una organización.

El contratista emitirá dos (02) tipos de alertas a la organización a fin de garantizar que se puedan implementar acciones preventivas a tiempo:

- Alertas mensuales: Se desarrollan informes mensuales de las vulnerabilidades MÁS CRÍTICAS en base al valor del CVSS.
- Alertas en demanda: Ante la nueva aparición de vulnerabilidades en la red, se emitirá una ALERTA TEMPRANA e inmediata para tomar acciones correctivas necesarias.

E. TECNOLOGÍA Y HERRAMIENTAS

- a) La metodología de trabajo debe alinearse con los estándares internacionales aceptados para las buenas prácticas de seguridad informática y seguridad de información, la asociación de control de auditoría, así como los controles establecidos por:
 - ISO 27000
 - NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment
 - OSSTMM (Open Source Security Testing Methodology Manual)
 - ISAAF (Information Systems Security Assessment Framework)
 - OWASP – Testing Guide v4.0
- b) El Contratista deberá brindar una plataforma web para la gestión de vulnerabilidades: dashboard para registro y seguimiento de las vulnerabilidades encontradas. Esta plataforma deberá contener como mínimo:
 - Top vulnerabilidad y hosts
 - Histórico del resultado de vulnerabilidades por nivel de severidad
 - Para cada vulnerabilidad se deberá considerar como mínimo:
 - Detalle de vulnerabilidad
 - Lista de host-IP
 - Indicador de vulnerabilidad (calificación)
 - CVSS

- Área Responsable
- Personal Responsable
- Activo afectado
- Acciones recomendadas o propuesta del E.H.
- Fecha Inicio
- Fecha Fin
- % avance
- Estado de la vulnerabilidad (de preferencia configurable por CAJA gris como en proceso, resuelto, implementado, en retest, cerrado)
- Planificación

F. ACOMPAÑAMIENTO EN EL PROCESO DE RESOLUCIÓN DE VULNERABILIDADES

El proveedor brindará una bolsa de 250 horas de sus consultores para realizar el acompañamiento en el proceso de resolución de vulnerabilidades. El acompañamiento en el proceso de resolución de vulnerabilidades comprende las siguientes actividades:

- Coordinar ventanas de tiempo para la realización de cambios en la infraestructura tecnológica y verificar que la vulnerabilidad identificada haya sido resuelta.
- Realizar la verificación inmediata de la resolución de la vulnerabilidad identificada para que pueda ser replicada en otros componentes de la red.
- Brindar asesoría constante para absolver dudas sobre el proceso de resolución de vulnerabilidades.
- A nivel de aplicaciones web y/o sistemas de información el proveedor deberá absolver dudas técnicas a nivel de líneas de código a modificar en los sistemas, especificando la recomendación específica sobre el lenguaje de programación y/o framework utilizado en la organización.
- Personal de la Oficina de Soporte e Infraestructura Tecnológica solicitará con dos (02) días de anticipación la reunión con el proveedor para el acompañamiento del proceso de resolución de vulnerabilidades. Estas reuniones podrán ser realizadas durante cualquier momento dentro del plazo del servicio.
- En caso se identifiquen vulnerabilidades que no puedan ser resueltas, el proveedor deberá brindar la solución al problema presentado y controles compensatorios que mitiguen el riesgo identificado.


Firmado digitalmente por
CHALCO MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:53:29 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:06:10 -05:00

G. DOCUMENTACIÓN E INFORMES

Se generarán informes personalizados para la entidad con toda la información obtenida de la actividad de evaluación y por cada test de penetración, así como las posibles soluciones que resuelvan o mitiguen cada incidencia detectada.

Nro.	ENTREGABLE
1	Plan de trabajo
2	02 Informes Técnicos (01 por cada revisión)
3	02 Informes Ejecutivos (01 por cada revisión)
4	Informes a demanda por cada aplicación solicitada a evaluar
5	02 informes de Ingeniería Social
6	12 informes mensuales de ciberseguridad (01 mensual)

El detalle de los documentos se detalla a continuación:

PLAN DE TRABAJO: El cual debe considerar como mínimo la siguiente información:

- Fases y etapas del servicio.
- El cronograma base con las principales actividades programadas para el servicio, la lista de las herramientas, equipos y/o productos que utilizará durante la ejecución.
- Indicadores de riesgos.
- Análisis, clasificación y priorización de las vulnerabilidades.
- Oportunidades de Mejora y conclusiones.
- Evolución de los riesgos.
- Definir los entregables por cada fase / etapa del servicio: Incluir identificación de software instalado (sistemas operativos, versiones, service pack, ptf) fuera de soporte de seguridad por parte del fabricante de la respectiva tecnología o service pack/ptf desactualizado respecto a último liberado.

Cabe señalar que el **Plan de Trabajo** deberá de ser presentado como máximo a los cinco (05) días siguientes a la suscripción del contrato.


INFORMES TÉCNICOS: Cada informe técnico deberá contener el detalle de todas las pruebas realizadas especificando su objetivo; herramientas utilizadas, metodologías, resultados obtenidos, así como las recomendaciones específicas para cada vulnerabilidad. Se debe confirmar que las medidas de seguridad implementadas por parte del área usuaria son las adecuadas y si son capaces de resistir un ataque.

- Técnicas utilizadas.
- Listado de vulnerabilidades encontradas, con el sustento de la existencia de las vulnerabilidades (evidencias concretas de los hallazgos) y la descripción de las herramientas que se utilizaron para su descubrimiento. (este informe no se deben incluir los falsos positivos).
- Acciones detalladas de la mitigación y/o solución para cada una de las vulnerabilidades a modo de guía de usuario con los correspondientes enlaces de referencia como sustento de la corrección y/o recomendación.
- Una matriz de riesgo basado en los hallazgos del escaneo de seguridad ejecutado.
- Avance en las correcciones de las vulnerabilidades
- En caso de retest el informe debe incluir el cierre de las vulnerabilidades remediadas y lo pendiente.
- Un Plan de acción preventivo y correctivo.

INFORME EJECUTIVO: Este documento debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados.

- Informe de las vulnerabilidades resueltas por la organización, en caso queden pendientes vulnerabilidades a resolver.
- El Informe de Propuestas y Recomendaciones, debe considerar como mínimo lo siguiente:
 - Propuesta de políticas, controles, estándares que ayuden a mitigar aquellas variantes de las vulnerabilidades anteriormente detectadas.
 - Propuesta de actualización tecnológica para superar las variantes de las vulnerabilidades detectadas.


modo digitalmente por CHALCO
ALDONADO Jose Luis FAU
1131373237 hard
otro: Doy V° B°
fecha: 31.07.2024 11:53:3e -05:00


modo digitalmente por
ERIANDEZ MAYTA Jonathan
FAU 20131373237 hard
otro: Doy V° B°
fecha: 31.07.2024 12:05:17 -05:00

- Recomendaciones para la mejora de la seguridad sobre las debilidades o falencias encontradas durante el análisis realizado.
- Recomendaciones respecto a herramientas que permitan la configuración, monitoreo y generación de alertas automáticas respecto a los incidentes de seguridad.
- Un Plan de acción preventivo y correctivo.

EL INFORME DE INGENIERÍA SOCIAL: Debe incluir el detalle de las pruebas realizadas, la prueba utilizada y los resultados obtenidos como: contraseñas, usuarios vulnerados, información personal obtenidas, etc.

EL INFORME DE CIBERSEGURIDAD: Debe incluir el riesgo de seguridad informática al que se encuentra expuesta la organización de manera mensual:

- Exposición en redes sociales, buscadores (Google, Bing, Shodan, etc) de la organización.
- Exposición de correos electrónicos en Foros, Grupos, etc de Internet.
- Suplantación de identidad en redes sociales: Facebook, Twitter, Instagram, LinkedIn.
- Búsqueda de información en portales tipo GITHUB, Pastebin.
- Monitoreo y búsqueda de información en la Deep/Dark Web.
- Consultas recurrentes de dominios similares a la organización.
- Alerta a proveedor de dominio y/o hosting en caso de detección de ataques tipo PHISHING.
- Alerta a buscadores de internet para misión de alertas de ataque en navegadores web.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:52:47 -05:00


Firmado digitalmente por
HERNANDEZ MAYTA Jonathan
Jose FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:05:25 -05:00

H. COMPONENTE CAPACITACIÓN

El proveedor brindará una capacitación de 24 horas (el cual se dará en 8 sesiones, cada una de 3 horas como máximo) sobre Pentesting sobre Infraestructura Tecnológica, la misma que se realizará en la fecha solicitada por el área usuaria y bajo los siguientes detalles:

- Cantidad de personas: De 6 a 10 personal de la OSIT.
- Las clases se realizarán en vivo, las cuales se grabarán y se compartirán con los asistentes.
- Se brindará una constancia de asistencia por la participación a la capacitación
- Temario:

Tema 1: Reconocimiento


- ✓ Búsqueda de direcciones IP públicas
 - ✓ Búsqueda de rangos de direcciones IP con WHOIS
 - ✓ Identificación de dominios y subdominios
 - ✓ Consulta de registros DNS
 - ✓ Google Hacking
 - ✓ Búsqueda de información en repositorios GITHUB
 - ✓ Búsqueda en repositorios públicos
 - ✓ Búsquedas avanzadas en redes sociales
 - ✓ Búsqueda de información en Deep Web
- Desarrollo de CTF (Capture The Flag) (02 horas)*

Tema 2: Escaneo

Escaneo de Puertos y Servicios:

- ✓ Definición del proceso de escaneo de puertos y servicios

 
Firmado digitalmente por CHALCO
HALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:53:56 -05:00

 
Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:05:33 -05:00

- ✓ Análisis del Three Way Handshake
- ✓ Definición y tipos de escaneo:
 - SYN SCAN
 - TCP FULL SCAN
 - IDLE SCAN
 - FIN SCAN
 - XMAS SCAN
- ✓ Técnicas de MAC SPOOFING
- ✓ Técnicas de SYN FLOOD
- ✓ Enumeración de información de Servidores
- ✓ Técnicas de identificación de sistema operativos
- Desarrollo de CTF (02 horas)*
- Escaneo de Vulnerabilidades:
 - ✓ Definición del proceso de escaneo y análisis de vulnerabilidades
 - ✓ Definición y categorización de vulnerabilidades
 - ✓ Identificación de vulnerabilidades con Nmap Script Engine (Nmap - NSE)
 - Vulnerabilidades en puertos y servicios de red
 - ✓ Identificación de vulnerabilidades con Tenable NESSUS
 - Vulnerabilidades en puertos y servicios de red
 - Vulnerabilidades en sistemas operativos sin autenticación
 - Vulnerabilidades en sistemas operativos con autenticación
 - ✓ Identificación de vulnerabilidades con Metasploit – Módulo Auxiliar
 - Reconocimiento del Framework Metasploit
 - Principales comandos y opciones del Framework Metasploit
 - Identificación de vulnerabilidades con módulo
- Auxiliar Desarrollo de CTF (02 horas)*

Tema 3: Ganando acceso Windows

Ganando Acceso Servidores:

- ✓ Definición del proceso de Ganar Acceso
- ✓ Definición de conceptos: exploit, payload, BoF
- ✓ Explotación de vulnerabilidades en Sistemas Operativos Windows
- ✓ Configuración y uso de METASPLOIT
 - Módulo Payload
 - Módulo Exploit
- ✓ Ataques de Hombre en el Medio (MitM)
- ✓ Ataques sobre el protocolo RDP
- ✓ Ataques sobre servicios:
 - Ataques sobre MSSQL y XP_CMDSHELL
 - Ataques sobre TOMCAT
 - Ataque sobre servicios POSTGRES
 - Ataques sobre LLMNR
 - Ataques sobre Active Directory
 - Ataque de ZEROLOGON
 - Ataque de Kerberoasting
 - Ataque de Golden Ticket
- ✓ Cracking de contraseñas LM, NTLM
 - Fuerza Bruta

- o Diccionario de Contraseña
- o Tablas Pre-Computadas

Desarrollo de CTF (02 horas)

Tema 4: Elevación de Privilegios en Sistemas Windows


- ✓ Explotación y vulnerabilidad en Kernel
- ✓ Explotación de vulnerabilidad a través de SUDO
- ✓ Explotación de SUID
- ✓ Explotación de archivo PASSWD
- ✓ Instalación de Backdoors en servicios:

Desarrollo de CTF (02 horas)

Tema 5: Manteniendo acceso

- ✓ Instalación de Backdoors en sistema operativo
- ✓ Instalación de Backdoors en servicios:
 - o RDP
 - o SMB
 - o HTTP
- ✓ Instalación de Backdoors en servidores web

Desarrollo de CTF (02 horas)


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:54:05 -05:00

9. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

9.1. REQUISITOS DEL CONTRATISTA

EQUIPAMIENTO

El proveedor deberá acreditar que cuenta con el equipamiento y recursos mínimos necesarios para garantizar un eficiente y oportuno servicio.


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:05:42 -05:00

EQUIPO DE TRABAJO

El Proveedor deberá contar con un equipo de trabajo: compuesto por un (1) jefe de proyecto, un (1) Consultor Senior en Seguridad de la Información, dos (02) consultores de seguridad de la información, un (1) consultor junior en seguridad de la información y un (1) consultor de apoyo. los siguientes perfiles.

Para la acreditación del cumplimiento de los perfiles: Se dará a través de copia simple de la constancia y/o certificados u otro documento que permita evidenciar fehacientemente el cumplimiento de los perfiles solicitados. Los mismos que deben ser presentados como parte de su propuesta técnica.

Cabe precisar que una persona no puede cubrir más de un rol como parte del equipo.

A) Jefe o Gerente del Proyecto: Un (1) Profesional.

Formación Académica: Copia simple del título de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

Certificaciones: Como mínimo cuatro (04) certificados oficiales VIGENTES, en cualquiera de las siguientes certificaciones de seguridad:

- PMP Project Management Professional
- ISO 27001 Lead Implementer
- ISO 27001 Lead Auditor
- CISSO (Certified Information Systems Security Officer)
- LCSPS (Lead Cybersecurity Professional Certificate)
- CISA (Certified Information Systems Auditor)
- CRISC (Certified in Risk and Information Systems Control)
- CISM (Certified Information Security Manager)
- Gerente Lider en Ciberseguridad ISO 27032

B) Consultor Sénior en Seguridad de la Información: Un (1) Profesional.

Formación Académica: Copia simple del título de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

Certificaciones: Como mínimo, seis (06) certificados oficiales VIGENTES, en cualquiera de las siguientes certificaciones de seguridad:


- LPT Master (Licensed Penetration Tester - Master)
- CPENT (Certified Penetration Testing Professional)
- CEH (Certified Ethical Hacker)
- CEH Practical (Certified Ethical Hacker)
- GPEN (GIAC Penetration Tester)
- GWAPT (Web Application Penetration Tester)
- CPTe (Certified Penetration Testing Engineer)
- CPEH (Certified Professional Ethical Hacker)
- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWE (Offensive Security Web Expert).
- CSWAE (Certified Web Secure Application Engineer).
- eJPT (eLearn Junior Penetration Testing)
- eWPT (eLearn Web Penetration Testing)
- eWPTX (eLearn Web Application Penetration Tester eXtreme)
- eCPPT (eLearn Certified Professional Penetration Tester)

C) Consultor en Seguridad de la Información: Dos (2) Profesionales

Formación Académica: Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

Certificaciones: Como mínimo, cuatro (04) certificados oficiales VIGENTES, en cualquiera de las siguientes certificaciones de seguridad:

- LPT Master (Licensed Penetration Tester - Master)
- ECSA (Council Certified Security Analyst)
- CEH (Certified Ethical Hacker)
- CEH Practical (Certified Ethical Hacker)


Firmado digitalmente por CHALCO
EDONADO Jose Luis FAU
31373237 hard
Ido: Doy V° B°
ha: 31.07.2024 11:54:13 -05:00



Firmado digitalmente por
RHANDEZ MAYTA Jonathan
win FAU 20131373237 hard
Ido: Doy V° B°
ha: 31.07.2024 12:05:53 -05:00

- GPEN (GIAC Penetration Tester)
- GWAPT (Web Application Penetration Tester)
- CPTe (Certified Penetration Testing Engineer)
- CPEH (Certified Professional Ethical Hacker)
- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWE (Offensive Security Web Expert).
- CSWAE (Certified Web Secure Application Engineer).
- eJPT (eLearn Junior Penetration Testing)
- eWPT (eLearn Web Penetration Testing)
- eCPPT(Certified Professional Penetration Tester)

D) Consultor Junior en Seguridad de la Información: Uno (1) Profesional

Formación Académica: Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 11:54:21 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Day V° B°
Fecha: 31.07.2024 12:06:03 -05:00

Certificaciones: Como mínimo, dos (02) certificados oficiales VIGENTES, en cualquiera de las siguientes certificaciones de seguridad:

- LPT Master (Licensed Penetration Tester - Master)
- ECSA (Council Certified Security Analyst)
- CEH (Certified Ethical Hacker)
- CEH Practical (Certified Ethical Hacker)
- GPEN (GIAC Penetration Tester)
- GWAPT (Web Application Penetration Tester)
- CPTe (Certified Penetration Testing Engineer)
- CPEH (Certified Professional Ethical Hacker)
- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWE (Offensive Security Web Expert).
- CSWAE (Certified Web Secure Application Engineer).
- eJPT (eLearn Junior Penetration Testing)
- eWPT (eLearn Web Penetration Testing)
- eCPPT(Certified Professional Penetration Tester)

E) Consultor de Apoyo: Un (1) Profesional

Formación Académica: Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

Certificaciones: Como mínimo, dos (02) certificados oficiales VIGENTES, en cualquiera de las siguientes certificaciones de seguridad:


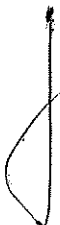
- LPT Master (Licensed Penetration Tester - Master)
- ECSA (Council Certified Security Analyst)
- CEH (Certified Ethical Hacker)

- CEH Practical (Certified Ethical Hacker)
- GPEN (GIAC Penetration Tester)
- GWAPT (Web Application Penetration Tester)
- CPTE (Certified Penetration Testing Engineer)
- CPEH (Certified Professional Ethical Hacker)
- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWE (Offensive Security Web Expert).
- CSWAE (Certified Web Secure Application Engineer).
- eJPT (eLearn Junior Penetration Testing)
- eWPT (eLearn Web Penetration Testing)
- eCPPT(Certified Professional Penetration Tester)

10. ENTREGABLES

Los entregables del proyecto serán los siguientes:

10.1. ENTREGABLE PARA EL COMPONENTE ETHICAL HACKING A NIVEL DE INFRAESTRUCTURA:

Entregable	Descripción	Plazo de Entrega
 1ER ETHICAL HACKING A NIVEL DE INFRAESTRUCTURA	<ul style="list-style-type: none"> • Acta de Inicio de Servicio, el mismo que se suscribirá al día siguiente de suscrito el contrato. • Acuerdo de confidencialidad. • Informe Técnico de Análisis de Vulnerabilidades, el cual debe contener como mínimo los siguientes documentos técnicos: <ul style="list-style-type: none"> ▫ Informe técnico de vulnerabilidades en infraestructura. ▫ Informe técnico de vulnerabilidades en aplicaciones y/o sistemas de información y/o web service. ▫ Informe técnico de vulnerabilidades en base de datos. • Informe Ejecutivo, el cual debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados. 	Cuarenta (40) días, contabilizados a partir del día de suscrito el Acta de Inicio.
 2DO ETHICAL HACKING A NIVEL DE INFRAESTRUCTURA	<ul style="list-style-type: none"> • 2do Informe Técnico de Análisis de Vulnerabilidades, el cual debe contener como mínimo los siguientes documentos técnicos: <ul style="list-style-type: none"> ▫ Informe técnico de vulnerabilidades en infraestructura. ▫ Informe técnico de vulnerabilidades en aplicaciones y/o sistemas de información y/o web service. ▫ Informe técnico de vulnerabilidades en base de datos. 	Ciento ochenta (180) días, contabilizados a partir del día de suscrito el Acta de Inicio.


firmado digitalmente por CHALCO
ALDONADO Jose Luis FAU
D131373237 hard
otivo, Doy V° B°
Fecha: 31.07.2024 11:54:42 -05:00

Entregable	Descripción	Plazo de Entrega
3ER ETHICAL HACKING A NIVEL DE INFRAESTRUCTURA	<ul style="list-style-type: none"> Informe Ejecutivo, el cual debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados. 3er Informe Técnico de Análisis de Vulnerabilidades, el cual debe contener como mínimo los siguientes documentos técnicos: <ul style="list-style-type: none"> Informe técnico de vulnerabilidades en infraestructura. Informe técnico de vulnerabilidades en aplicaciones y/o sistemas de información y/o web service. Informe técnico de vulnerabilidades en base de datos. Informe Ejecutivo, el cual debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados. 	Trescientos cincuenta (350) días, contabilizados a partir del día de suscrito el Acta de Inicio.

10.2. ENTREGABLE PARA EL COMPONENTE DE ETHICAL HACKING DE APLICACIONES A DEMANDA


firmado digitalmente por
ERIKANDER MAYTA Jonathan
D131373237 hard
otivo, Doy V° B°
Fecha: 31.07.2024 12:06:23 -05:00

Entregable	Descripción	Plazo de Entrega
ETHICAL HACKING DE APLICACIONES A DEMANDA	<ul style="list-style-type: none"> Informe del Análisis de Vulnerabilidades a demanda realizado, el cual debe contener como mínimo los siguientes documentos técnicos: <ul style="list-style-type: none"> Informe técnico de vulnerabilidades en infraestructura. Informe técnico de vulnerabilidades en aplicaciones y/o sistemas de información y/o web service. Informe técnico de vulnerabilidades en base de datos. Informe Ejecutivo, el cual debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados. 	A demanda, se debe considerar la entrega de la documentación solicitada como máximo a los cinco días de haberse culminado la ejecución del análisis solicitado por personal de la OSIT.

10.3. ENTREGABLE PARA EL COMPONENTE DE PRUEBAS DE INGENIERIA SOCIAL:

Entregable	Descripción	Plazo de Entrega
1ERA PRUEBAS DE INGENIERIA SOCIAL	<ul style="list-style-type: none"> 1er Informe de Ingeniería Social, el cual debe contener como mínimo los siguientes documentos técnicos: 	Cien (100) días, contabilizados a partir del día de suscrito el Acta de Inicio.



	<ul style="list-style-type: none"> ▪ Detalle de las pruebas realizadas y los resultados obtenidos (con las evidencias) a nivel de phishing. ▪ Detalle de las pruebas realizadas y los resultados obtenidos (con las evidencias) a nivel de revisión de escritorios limpios. ▪ Recomendaciones y propuesta de políticas al respecto. 	
2DA PRUEBAS DE INGENIERIA SOCIAL	<ul style="list-style-type: none"> • 2do Informe de Ingeniería Social, el cual debe contener como mínimo los siguientes documentos técnicos: <ul style="list-style-type: none"> ▪ Detalle de las pruebas realizadas y los resultados obtenidos (con las evidencias) a nivel de phishing. ▪ Detalle de las pruebas realizadas y los resultados obtenidos (con las evidencias) a nivel de revisión de escritorios limpios. ▪ Recomendaciones y propuesta de políticas al respecto. 	Doscientos (200) días, contabilizados a partir del día de suscrito el Acta de Inicio.

10.4. PARA EL COMPONENTE DE EJERCICIOS DE CIBERVIGILANCIA:



Entregable	Descripción	Plazo de Entrega
ETHICAL HACKING DE APLICACIONES A DEMANDA	<ul style="list-style-type: none"> • Informe de ciberseguridad mensual, el cual debe contener como mínimo la siguiente información: <ul style="list-style-type: none"> ▪ Exposición en redes sociales, buscadores (Google, Bing, Shodan, etc) de la organización. ▪ Exposición de correos electrónicos en Foros, Grupos, etc de Internet. ▪ Suplantación de identidad en redes sociales: Facebook, Twitter, Instagram, LinkedIn. ▪ Búsqueda de información en portales tipo GITHUB, Pastebin. ▪ Monitoreo y búsqueda de información en la Deep/Dark Web. ▪ Consultas recurrentes de dominios similares a la organización. ▪ Alerta a proveedor de dominio y/o hosting en caso de detección de ataques tipo PHISHING. ▪ Alerta a buscadores de internet para misión de alertas de ataque en navegadores web. 	Hasta los dos (02) días siguientes de culminado el mes de servicio (1 informe mensual / 12 informes durante todo el contrato).

Cada informe técnico de vulnerabilidades, debe considerar como mínimo lo siguiente:

- ❖ Detalle de todas las pruebas realizadas especificando su objetivo; herramientas utilizadas, metodologías, resultados obtenidos, vulnerabilidades encontradas y las propuestas de remediación, no se deberá incluir falsos positivos.

- ❖ Listado de vulnerabilidades encontradas, con el sustento de la existencia de las vulnerabilidades y la descripción de las herramientas que se utilizaron para su descubrimiento. (este informe no se deben incluir los falsos positivos).
- ❖ Una matriz de riesgo basado en los hallazgos del escaneo de seguridad ejecutado.
- ❖ Recomendaciones para la subsanación de todas las vulnerabilidades detectadas.
- ❖ Un Plan de acción preventivo y correctivo.



Cabe precisar que, para el informe ejecutivo, debe considerar información mínima necesaria que permita evidenciar los riesgos y consecuencias de no subsanar o solucionar los riesgos identificados.

- ❖ Informe Ejecutivo.
- ❖ Acta de compromiso del Informe de Resolución de vulnerabilidades.

11. LUGAR Y PLAZO DE LA PRESTACIÓN



11.1. LUGAR

El servicio se brindará en la sede central del **MINSA**, pudiendo desarrollarse las actividades de manera remota, es decir, desde las instalaciones del proveedor y aquellas evaluaciones que se requiera realizar de manera presencial, se deberá realizar las coordinaciones para el acceso a las oficinas.

11.2. PLAZO

El servicio tendrá un periodo de duración de trescientos sesenta y cinco (365) días calendario, contabilizados a partir del día siguiente de haber suscripto el contrato o de la recepción de la notificación de la Orden de Servicio.

12. FORMA DE PAGO

El pago se realizará en doce (12) armadas, de acuerdo al siguiente detalle:

Pago	Descripción	Detalle
Primer pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 1er Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura y el 1er Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Segundo pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 2do Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.


Firmado digitalmente por CHALCO
ALDONADO Jose Luis FAU
9131373237 hard
otivo: Day V° B°
echa: 31.07.2024 11:55:13 -05:00


Firmado digitalmente por
SERRANDEZ KATYA Jonathan
Fau FAU 20131373237 hard
otivo: Day V° B°
echa: 31.07.2024 12:07:35 -05:00

Pago	Descripción	Detalle
Tercer pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 3er Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Cuarto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 4to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, el 1er Informe de Ingeniería Social solicitado en el numeral 10.3. y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Quinto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 5to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	5% del monto total del contrato.
Sexto pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 2do Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura, el 6to Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Séptimo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 7mo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia, el 2do Informe de Ingeniería Social solicitado en el numeral 10.3. y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.
Octavo pago	Previa conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 8avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.


 Firmado digitalmente por CHALCO
 TALDOVADO Jose Luis FAU
 0101373237 hard
 fecha: 31.07.2024 11:56:27 -05:00


 Firmado digitalmente por
 ERNANDEZ MAYTA Jonathan
 Juan FAU 20131373237 hard
 fecha: 31.07.2024 12:09:13 -05:00

Pago	Descripción	Detalle
Noveno pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 9no Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Décimo pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 10mo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	8% del monto total del contrato.
Onceavo pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el 11avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	7% del monto total del contrato.
Doceavo pago	Prevía conformidad técnica emitida por la Oficina de Soporte e Infraestructura Tecnológica adjuntando el entregable denominado 3er Ethical Hacking a Nivel de Infraestructura detallado en el numeral 10.1. Entregable para el Componente Ethical Hacking a Nivel de Infraestructura, el 12avo Informe de ciberseguridad solicitado en el numeral 10.4. Entregable para el Componente de Ejercicios de Cibervigilancia y de corresponder el entregable denominado Ethical Hacking de Aplicaciones a Demanda, solicitado en el numeral 10.2. descritos en el numeral 10 ENTREGABLES.	10% del monto total del contrato.

13. CONFORMIDAD

La conformidad de la prestación será emitida en un plazo no mayor de siete (07) días calendario, en base a la forma de pago establecida en el numeral 13. FORMA DE PAGO, para dicho efecto la Oficina de Soporte e Infraestructura Tecnológica, deberá firmar en señal de conformidad el "Acta de Conformidad del Servicio". De existir observaciones, será notificado a EL CONTRATISTA, estableciendo un plazo para que subsane, el cual no podrá ser menor de (02) ni mayor de ocho (08) días calendario, dependiendo de la complejidad.

14. PENALIDADES

En caso de retraso injustificado de **EL CONTRATISTA** en la ejecución de las prestaciones (Inicio e Implementación del Servicio) objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde:

F= 0.25 para plazos mayores a cuarenta y cinco (45) días o;

F= 0.40 para plazos menores o iguales a cuarenta y cinco (45) días.

Para efectos del cálculo de la penalidad diaria, se considerará el monto y plazo total de ejecución del contrato vigente.

Se considera justificado el retraso, cuando **EL CONTRATISTA** acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

14.1. OTRAS PENALIDADES

De conformidad con lo estipulado en el Art. 163° del Reglamento de la Ley de Contrataciones y Adquisiciones del Estado, aprobado mediante D.S. 344-2018-EF y sus modificatorias (D.S. N° 377-2019-EF y D.S. N° 168-2020-EF) sin perjuicio de la aplicación de penalidades que estipula el Art. 161° del citado instrumento legal.


Esta penalidad será deducida de los pagos establecidos, según corresponda al período en el cual ocurrió la afectación del servicio. Teniendo en consideración las condiciones generales, al contratista se le aplicará las penalidades, según los siguientes puntos:


Firmado digitalmente por CHALCO MALDONADO Jose Lis FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:55:37 -05:00


Firmado digitalmente por FERNANDEZ MAYTA Jonathan Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:10:25 -05:00

N°	APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Penalidad por demora o retraso en la ejecución del análisis de vulnerabilidades externo: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la ejecución del servicio de análisis de vulnerabilidades externo.</i>	Monto total de la penalidad = 50% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). (* La fracción acumulada será considerada como un (01) día.	El total de días de demora se contabiliza desde la finalización del plazo definido para la ejecución del análisis hasta que el contratista informe de la culminación del mismo.
2	Penalidad por demora o retraso en la ejecución del análisis de vulnerabilidades interno: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la ejecución del servicio de análisis de vulnerabilidades externo.</i>	Monto total de la penalidad = 50% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). (* La fracción acumulada será considerada como un (01) día.	El total de días de demora se contabiliza desde la finalización del plazo definido para la ejecución del análisis hasta que el contratista informe de la culminación del mismo.
3	Penalidad por demora o retraso en la presentación de	Monto total de la penalidad = 30% x (valor de la UIT) x T <u>Donde:</u>	El total de días de demora se contabiliza desde la finalización


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 11:55:47 -05:00


Firmado digitalmente por
FERNANDEZ MAYTA Jonathan
Edwin FAU 20131373237 hard
Motivo: Doy V° B°
Fecha: 31.07.2024 12:15:36 -05:00

N°	APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
	entregables: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la presentación de los ENTREGABLES.</i>	UIT: Unidad Impositiva Tributaria $T = \text{Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*)}$. <i>(*) La fracción acumulada será considerada como un (01) día.</i>	del plazo definido para la entrega de los entregables hasta que el contratista presente los entregables al MINSA.
4	Penalidad por la demora en la entrega del Plan de Trabajo.	Monto total de la penalidad = $20\% \times (\text{valor de la UIT}) \times T$ <u>Donde:</u> UIT: Unidad Impositiva Tributaria $T = \text{Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*)}$. <i>(*) La fracción acumulada será considerada como un (01) día.</i>	El total de días de demora se contabiliza desde la finalización del plazo definido para la entrega del Plan de Trabajo hasta que el contratista presente los entregables al MINSA.
5	Penalidad por generar la indisponibilidad del sistema y/o servicios del MINSA analizado, por cada ocurrencia y/o servicio afectado.	Monto total de la penalidad = $50\% \times (\text{valor de la UIT}) \times \text{OCURRENCIA}$ <u>Donde:</u> UIT: Unidad Impositiva Tributaria	La penalidad descrita en la tabla se determinará según informe de la Oficina de Soporte e Infraestructura Tecnológica -OSIT

Definición

Cuando la sumatoria de los incumplimientos exceda el monto máximo de la penalidad, el Ministerio de Salud podrá resolver el contrato por incumplimiento.

Todo incumplimiento de parte del contratista, será informado por la Oficina General de Tecnologías de la Información a la Oficina de Abastecimiento para las gestiones administrativas correspondientes.

15. CLÁUSULA ANTICORRUPCIÓN

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

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

Además, **EL CONTRATISTA** se compromete a:

- i) Comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento
- ii) Adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.


El incumplimiento de las obligaciones establecidas en estas cláusulas, durante la ejecución contractual, da el derecho a la Entidad correspondiente a resolver automáticamente y de pleno derecho el contrato, bastando para tal efecto que la Entidad remita una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiera lugar.


Firmado digitalmente por CHALCO
ALDONADO Jose Luis FAU
3131373237 hard
otivo: Doy V° B°
Fecha: 31.07.2024 11:59:57 -05:00



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

16. RESPONSABILIDAD POR VICIOS OCULTOS


Firmado digitalmente por
ERNAÑANDEZ MAYTA Jonathan
Firm FAU 20131373237 hard
otivo: Doy V° B°
Fecha: 31.07.2024 12:16:50 -05:00



El contratista es responsable por la calidad del servicio ofrecida y por los vicios ocultos del servicio ofrecido por un plazo no menor de trescientos sesenta y cinco (365) días calendario, contados a partir de la conformidad otorgada por el MINSA de acuerdo al artículo 40° de la Ley de Contrataciones del Estado.

17. RESOLUCION DE CONTRATO Y/U ORDEN

En caso de incumplimiento de obligaciones contractuales el Ministerio de Salud, procederá a resolver el contrato y/u orden, tomando como referencia el procedimiento establecido en los artículos 164° y 165° del Reglamento de la Ley de Contrataciones del Estado.

18. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN


En virtud del cumplimiento de la Resolución Ministerial N° 074-2017/MINSA, que aprueba la Directiva Administrativa N° 227-MINSA/2017/OGTI correspondiente a la "Organización del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud", de la Ley de Protección de Datos Personales y del Sistema de Gestión de Seguridad de la Información, implementado en la Institución, acepto y reconozco que por motivo de mi condición laboral con el Ministerio de Salud y por el trabajo que presto para esta Institución tengo acceso a tecnología, documentos, datos, especificaciones, métodos, procesos y en general información **CONFIDENCIAL**, en tal virtud, por este medio me obligo a no divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir, sin la autorización expresa y por escrito del Ministerio de Salud, la información y documentación a que tengo acceso. Por lo que declaro haber leído y tener conocimiento de los documentos de gestión que involucran mi función y desenvolvimiento en el Ministerio de Salud, el Reglamento de Organización y Funciones del Ministerio de Salud - ROF, La Ley 27815 – Ley de Ética de la Función Pública y demás normativa que corresponde, publicados en la página web institucional.

En caso de incumplimiento, me someto a las responsabilidades de índole administrativa, penal y civil conforme a Ley.

Las obligaciones y derechos inmersos en el presente acuerdo de confidencialidad estarán vigentes a partir de la fecha de firma del vínculo con la Institución, durante el tiempo que dure esta relación y

después de la fecha en que se haya dado por terminada la relación laboral, sin importar la razón de la misma.

A los efectos previstos en este Compromiso, se define como "Información confidencial" a toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, que sea suministrada y/o comunicada por el Ministerio de Salud, mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.



Firmado digitalmente por
"FERNANDEZ MAYTA, Jonathan
Sobrin FAU 20131373237 hand
Motivo: Soy el autor del documento
Fecha: 31.07.2024 12:17:05 -05:00

En el supuesto de que, previamente a la firma del presente compromiso, el suscrito hubiera tenido acceso a la información de la institución, aquella será considerada también, a todos los efectos previstos en el presente documento, como información confidencial, salvo aquella que expresamente sea calificada por el Ministerio como información de libre uso o divulgación.

19. PERSONAL DE LA OFICINA USUARIA RESPONSABLE DE LAS COORDINACIONES

AREA	APELLIDOS Y NOMBRES	CORREO	TELÉFONO
Usuaría	José Chalco Maldonado	jchalcom@minsa.gob.pe	3156600 anexo: 3077
Usuaría	Jonathan Fernández Mayta	jfernandez@minsa.gob.pe	3156600 anexo: 3076


Firmado digitalmente por CHALCO
MALDONADO Jose Luis FAU
20131373237 hand
Motivo: Soy el autor del documento
Fecha: 31.07.2024 11:56:07 -05:00


Firmado digitalmente por GONZALEZ
ESCOBEDO Nieves Vanessa FAU
20131373237 soft
Motivo: Soy el autor del documento
Fecha: 31.07.2024 14:52:06 -05:00

Importante

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

20. REQUISITOS DE CALIFICACIÓN⁴

A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1	CALIFICACIONES DEL PERSONAL CLAVE
A.1.1	FORMACIÓN ACADÉMICA
	<u>Requisitos:</u> a) Un (01) Jefe o Gerente de Proyecto: Copia simple del título de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software. b) Un (01) Consultor Senior en Seguridad de la Información: Copia simple del título de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

⁴ La Entidad puede adoptar solo los requisitos de calificación contenidos en el presente capítulo, de acuerdo al artículo 28 del Reglamento. Los requisitos de calificación son fijados por el área usuaria en el requerimiento.



 Firmado digitalmente por
 ERNANDEZ MAYTA Jonathan
 .dwn FAU 20131373237 hard
 folio: Dey V° B°
 fecha: 31.07.2024 12:17:21 -05:00



 Firmado digitalmente por CHALCO
 MALDONADO Jose Luis FAU
 20131373237 hard
 folio: Dey V° B°
 fecha: 31.07.2024 11:56:19 -05:00

c) **Dos (02) Consultor en Seguridad de la Información:** Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

d) **Un (01) Consultor Junior en Seguridad de la Información:** Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

e) **Un (01) Consultor de Apoyo:** Copia simple del título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informático o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software.

Acreditación:

Los Grados o Títulos solicitados, 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 los grados o títulos requeridos no se encuentren inscritos en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

Importante

Se debe aceptar las diferentes denominaciones utilizadas para acreditar la carrera profesional requerida, aun cuando no coincida literalmente con aquella prevista en las bases (por ejemplo, Ingeniería Ambiental, Ingeniería en Gestión Ambiental, Ingeniería y Gestión Ambiental u otras denominaciones).

A.1.2

EXPERIENCIA DEL PERSONAL CLAVE

a) **Un (01) Jefe o Gerente de Proyecto:** Experiencia laboral mínima de cinco (05) años como Jefe y/o Gerente y/o Gestor de Servicio y/o Gestor de Proyectos en Servicio de Hacking Ético y/o Servicio de Pentesting y/o Servicio de Análisis de Código Fuente y/o Servicio de Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o Servicio de Test de Intrusión y/o Servicio de Test de Vulnerabilidades y/o Servicio de Test de Penetración y/o Provisión de sistemas de monitoreo intraoperativo y/o Servicio de Gestión de Riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del título profesional.

b) **Un (01) Consultor Senior en Seguridad de la Información:** Experiencia laboral mínima de cinco (05) años como Consultor Senior en Servicio de Hacking Ético y/o Servicio de Pentesting y/o Servicio de Análisis de Código Fuente y/o Servicio de


ado digitalmente por CHALCO
DONADO Jose Luis FAU
11373237 hard
v0: Day V B
14: 31.07.2024 11:56:28 -05:00


ado digitalmente por
NANDEZ MAYTA Jonathan
in FAU 20131373237 hard
v0: Day V B
14: 31.07.2024 12:17:31 -05:00

Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o Servicio de Test de Intrusión y/o Servicio de Test de Vulnerabilidades y/o Servicio de Test de Penetración y/o Provisión de sistemas de monitoreo intraoperativo y/o Servicio de Gestión de Riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del título profesional.

c) **Dos (02) Consultor en Seguridad de la Información:** Experiencia laboral mínima de tres (03) años como Consultor en Seguridad de la Información en Servicio de Hacking Ético y/o Servicio de Pentesting y/o Servicio de Análisis de Código Fuente y/o Servicio de Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o Servicio de Test de Intrusión y/o Servicio de Test de Vulnerabilidades y/o Servicio de Test de Penetración y/o Provisión de sistemas de monitoreo intraoperativo y/o Servicio de Gestión de Riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del título profesional.

d) **Un (01) Consultor Junior en Seguridad de la Información:** Experiencia laboral mínima de dos (02) años como Consultor Junior y/o Consultor en Seguridad de la Información en Servicio de Hacking Ético y/o Servicio de Pentesting y/o Servicio de Análisis de Código Fuente y/o Servicio de Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o Servicio de Test de Intrusión y/o Servicio de Test de Vulnerabilidades y/o Servicio de Test de Penetración y/o Provisión de sistemas de monitoreo intraoperativo y/o Servicio de Gestión de Riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del título profesional.

e) **Un (01) Consultor de Apoyo:** Experiencia laboral mínima de dos (02) años como Consultor en Seguridad de la Información en Servicio de Hacking Ético y/o Servicio de Pentesting y/o Servicio de Análisis de Código Fuente y/o Servicio de Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o Servicio de Test de Intrusión y/o Servicio de Test de Vulnerabilidades y/o Servicio de Test de Penetración y/o Provisión de sistemas de monitoreo intraoperativo y/o Servicio de Gestión de Riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del título profesional.

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

Acreditación:

La experiencia del personal 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 clave propuesto.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del profesional, 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 profesional 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 de los profesionales, 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 profesional corresponden con la función propia del cargo o puesto requerido en las bases.

B EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/. 500,000.00 (Quinientos Mil y 00/100 nuevos soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 60,000 (Sesenta 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Servicio de Hacking Ético y/o
- Servicio de Pentesting y/o
- Servicio de Análisis de Código Fuente y/o
- Servicio de Revisión y Monitoreo de Seguridad para el Desarrollo del Software y/o
- Servicio de Test de Intrusión y/o
- Servicio de Test de Vulnerabilidades y/o
- Servicio de Test de Penetración y/o Pentesting y/o
- Provisión de sistemas de monitoreo intraoperativo
- Servicio de Gestión de Riesgos de TI.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁵, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de

 
ado digitalmente por CHALCO
DONADIO JHON LUIS FAU
H373237 hard
vo: Doy V° B°
ta: 31.07.2024 11:56:37 -05:00

 
ado digitalmente por
SHANDEZ MAYTA Jonathan
m FAU 20131373237 hard
vo: Doy V° B°
ta: 31.07.2024 12:20:34 -05:00

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".


Firmado digitalmente por CHALCO
FALDONADO Jose Luis FAU
0131373237 hard
Motivo: Soy V° B°
Fecha: 31.07.2024 11:56:48 -05:00


Firmado digitalmente por
ERBANDEZ MAYTA Jonathan
Iwin FAU 20131373237 hard
Motivo: Soy V° B°
Fecha: 31.07.2024 12:20:46 -05:00

presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

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


Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad

Importante

- Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.
- En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".


Firmado digitalmente por GONZALEZ
ESCOBEDO HERRERA Vanessa FAU
20131373237 soft
Motivo: Soy el autor del documento
Fecha: 31.07.2024 14:51:45 -05:00

Importante

- Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.
- El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento de algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.
- Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.

CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<p>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> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i= Oferta <i>P_i</i>= Puntaje de la oferta a evaluar <i>O_i</i>=Precio i <i>O_m</i>= Precio de la oferta más baja <i>PMP</i>=Puntaje máximo del precio</p> <p style="text-align: right;">100 puntos</p>

Importante

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

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación del servicio de ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE SALUD, que celebra de una parte EL MINISTERIO DE SALUD, en adelante LA ENTIDAD, con RUC N°20131373237 con domicilio legal en AV. SALAVERRY N°801- JESÚS MARÍA- 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1** para la contratación del servicio de ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE SALUD, que celebra de una parte EL MINISTERIO DE SALUD, 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 ANÁLISIS DE VULNERABILIDADES SOBRE LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE SALUD, que celebra de una parte EL MINISTERIO DE SALUD.

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 PAGO¹³

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES en DOCE PAGOS PARCIALES, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

¹³ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de Trescientos Sesenta y cinco (365) días calendarios contabilizados a partir del día siguiente de haber suscrito el contrato o de la recepción de la notificación de la orden de servicio.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

"De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesorio como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente:

"De fiel cumplimiento por prestaciones accesorias: [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."

Importante

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00). Dicha excepción también aplica a 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 no supere el monto señalado anteriormente.

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 en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por LA OFICINA DE SOPORTE E INFRAESTRUCTURA TECNOLÓGICA en el plazo máximo de SIETE (7) DÍAS de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no 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 UN (1) AÑO contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA SEGUNDA: PENALIDADES

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

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

Donde:

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

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

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante

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

OTRAS PENALIDADES:

N°	APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Penalidad por demora o retraso en la ejecución del análisis de vulnerabilidades externo: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la ejecución del servicio de análisis de vulnerabilidades externo.</i>	Monto total de la penalidad = 50% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). <i>(*) La fracción acumulada será considerada como un (01) día.</i>	El total de días de demora se contabiliza desde la finalización del plazo definido para la ejecución del análisis hasta que el contratista informe de la culminación del mismo.
2	Penalidad por demora o retraso en la ejecución del análisis de vulnerabilidades interno: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la ejecución del servicio de análisis de vulnerabilidades</i>	Monto total de la penalidad = 50% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). <i>(*) La fracción acumulada será considerada como un (01) día.</i>	El total de días de demora se contabiliza desde la finalización del plazo definido para la ejecución del análisis hasta que el contratista informe de la culminación del mismo.

N°	APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
	externo		
3	Penalidad por demora o retraso en la presentación de entregables: <i>Se aplicará penalidad por cada fracción u día de incumplimiento que genere la demora en la presentación de los ENTREGABLES.</i>	Monto total de la penalidad = 30% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). (* La fracción acumulada será considerada como un (01) día.	El total de días de demora se contabiliza desde la finalización del plazo definido para la entrega de los entregables hasta que el contratista presente los entregables al MINSA.
4	Penalidad por la demora en la entrega del Plan de Trabajo.	Monto total de la penalidad = 20% x (valor de la UIT) x T <u>Donde:</u> UIT: Unidad Impositiva Tributaria T = Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). (* La fracción acumulada será considerada como un (01) día.	El total de días de demora se contabiliza desde la finalización del plazo definido para la entrega del Plan de Trabajo hasta que el contratista presente los entregables al MINSA.
5	Penalidad por generar la indisponibilidad del sistema y/o servicios del MINSA analizado, por cada ocurrencia y/o servicio afectado.	Monto total de la penalidad = 50% x (valor de la UIT) x OCURRENCIA <u>Donde:</u> UIT: Unidad Impositiva Tributaria	La penalidad descrita en la tabla se determinará según informe de la Oficina de Soporte e Infraestructura Tecnológica -OSIT

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

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

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS¹⁴

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:

¹⁴ 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: [.....]

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

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

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

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁵.

¹⁵ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS



ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
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 ¹⁶		Sí	No
Correo electrónico :			

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios¹⁷

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.

¹⁶ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁷ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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**ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1**

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 ¹⁸		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ¹⁹		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ²⁰		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.

¹⁸ En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁹ Ibídem.

²⁰ Ibídem.

2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios²¹

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.

²¹ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente.-

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

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
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 **[CONSIGNAR EL OBJETO DE LA CONVOCATORIA]**, 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

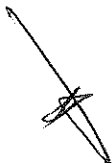
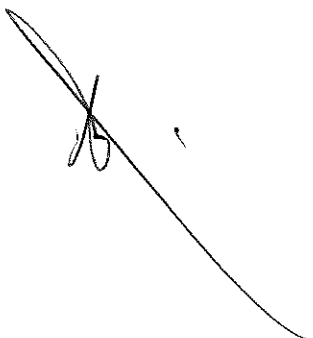
DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
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 [CONSIGNAR EL PLAZO OFERTADO].

[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
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1**

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] [%]²²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²³

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁴

[CONSIGNAR CIUDAD Y FECHA]

²² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²³ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

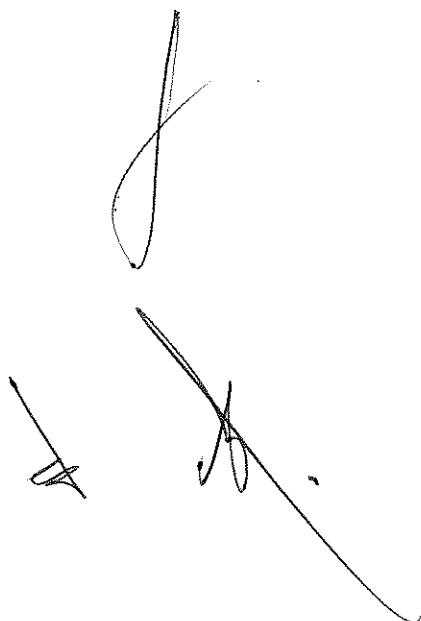
²⁴ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....
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.

Handwritten signatures and marks, including a large stylized signature and several smaller marks.

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] 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.*
- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*
Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
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 ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
1										
2										
3										
4										

²⁵ 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.

²⁶ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

²⁷ 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".

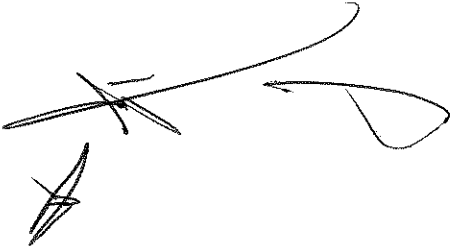
²⁸ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁹ 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.

³⁰ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
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° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 11

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/>.
- Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.

ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 011-2024-MINSA-1
Presente. -

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

