BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES
BASES INTEGRADAS

LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES

"ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD - SIEM"

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

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

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

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

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

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

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante
• *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.* • *En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.* • *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento

de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*

  Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.

- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante
En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a cien mil Soles (S/ 100,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia

de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

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

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).* *2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.* *De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-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 bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	**SUPERINTENDENCIA NACIONAL DE MIGRACIONES**
RUC N°	:	***20551239692***
Domicilio legal	:	Av. España N° 734 Breña - Lima
Teléfono:	:	(511) 200-1000
Correo electrónico:	:	isilva@migraciones.gob.pe; jchoque@migraciones.gob.pe; smarcelo@migraciones.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la **ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM.**

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado por la Oficina General de Administración y Finanzas mediante FORMATO 02 N° 018-2020-AE de fecha 11 de setiembre de 2020.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Diretamente Recaudados – RDR

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. MODALIDAD DE EJECUCIÓN

LLAVE EN MANO

1.7. DISTRIBUCIÓN DE LA BUENA PRO

NO APLICA

1.8. ALCANCES DEL REQUERIMIENTO

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

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en el plazo de se detalla como Prestación Principal y Prestación Accesoria, según se detalla en concordancia con lo establecido en el expediente de contratación.

	ACTIVIDAD	PLAZO DEL CONTRATISTA
PRESTACIÓN PRINCIPAL	El CONTRATISTA realizará la **entrega de bienes.** Carta adjuntando copias de las guías de remisión y "Acta de Recepción"	Hasta los cuarenta y cinco (45) días calendario, contados a partir del día siguiente de suscrito el contrato.
	El CONTRATISTA realizará la **instalación y configuración.** Entrega del Informe final" a la Superintendencia Nacional de Migraciones, según lo indicado en el numeral **7.1**.	Hasta los sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato.
PRESTACIÓN ACCESORIA	Capacitación.	Hasta los ciento ochenta (180) días calendario, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*".
	Mantenimiento Preventivo y Soporte Técnico.	El mantenimiento preventivo debe realizarlo el contratista como mínimo una (01) vez al año durante el periodo de vigencia de la garantía (03 años). El soporte técnico debe brindarse en modalidad 7x24x 365 durante el periodo de vigencia de la garantía (03 años). . Ambas actividades inician a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.
	Seguridad gestionada	Se realizará durante el tiempo que dure la garantía, tres (03) años, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 10.00 (Diez y 00/100 soles) de forma directa en la Oficina de Tesorería de la Oficina General de Administración y Finanzas, ubicado en la Av. España N° 734 Breña, Piso 5to.- Lima.

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

1.11. BASE LEGAL

- ✓ Ley de Presupuesto del Sector Público para el Año Fiscal 2019 – Ley N° 30879.
- ✓ Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2019 – Ley N° 30880.
- ✓ Ley N° 30225, Ley de Contrataciones del Estado, modificado mediante el Decreto Legislativo N° 1341.
- ✓ Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento, modificado mediante el Decreto Legislativo N° 1444.
- ✓ Directivas del OSCE.
- ✓ Ley Nº 27444, Ley del Procedimiento Administrativo General.
- ✓ Ley Nº 27806, Ley de Transparencia y de Acceso a la Información Pública.
- ✓ Decreto Supremo N° 304-2012-EF, TUO de la Ley General del Sistema Nacional del Presupuesto.
- ✓ Decreto Supremo Nº 008-2008-TR, Reglamento de la Ley MYPE.
- ✓ Código Civil.
- ✓ Ley N° 30353 (Ley que crea el Registro de Deudores de Reparaciones Civiles - REDERECI).
- ✓ Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley del Gobierno Digital
- ✓ Decreto Supremo N° 008-2020-SA, Declara en Emergencia Sanitaria el Estado Peruano desde el 16 de marzo de 2020.
- ✓ Decreto Supremo N° 044-2020-PCM, donde se declara el Estado de Emergencia Nacional, por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19, precisados por los Decretos Supremos N° 045-2020-PCM y N° 046-2020-PCM.
- ✓ Decreto Supremo N° 103-2020-EF Decreto Supremo que establece disposiciones reglamentarias para la tramitación de los procedimientos de selección que se reinicien en el marco del Texto Único Ordenado de la Ley Nº 30225.
- ✓ Decreto Supremo N° 020-2020-SA, declara la prórroga de Emergencia Sanitaria declarada por Decreto Supremo N° 008-2020-SA.por (90) noventa días a partir del 10 de junio de 2020.

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 documentos[1], la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

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

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

Advertencia
De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[2] 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.

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

[2] 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/

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo Nº 2)**

d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo Nº 3**).

e) Matriz de Cumplimiento de punto por punto, para lo cual añadirá una columna en cada característica solicitada donde debe colocar el número de folio que evidencie el cumplimiento de lo solicitado a través de referencias a datasheets o manuales o links o imágenes los cuales se deben adjuntar, (ver modelo adjunto: MATRIZ DE CUMPLIMIENTO DE CARACTERÍSTICA TÉCNICAS MINIMAS DE LA HERRAMIENTA DE GESTION DE EVENTOS E INFORMACION DE SEGURIDAD).

f) Declaración Jurada con el listado del equipamiento -que da cumplimiento a la Matriz de cumplimiento punto por punto- indicando marca y modelo, y en el que se indique que los equipos son vigentes tecnológicamente y que son el último modelo lanzado por el fabricante al mercado. La Declaración Jurada debe estar respaldada con una carta del fabricante.[3]

g) Declaración jurada de plazo de entrega. **(Anexo Nº 4)**[4]

h) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo Nº 5**)

i) El precio de la oferta en SOLES debe registrarse directamente en el formulario electrónico del SEACE.

Adicionalmente, se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios.

En el caso de procedimientos convocados a suma alzada únicamente se debe adjuntar el Anexo N° 6, cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.

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

j) Declaración Jurada indicado que cuenta con un Centro de Operaciones de Seguridad - SOC propio en el territorio nacional. (indicar dirección).

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa

[3] Absolución a la consulta N° 10, 58,125.

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

Advertencia
El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato.CARTA FIANZA.
b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso. CARTA FIANZA.
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 – PIDE[5] 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) Detalle de los precios unitarios del precio ofertado[6].
i) Presentar una estructura de costos diferenciada para la prestación principal y para las prestaciones accesorias.[7]

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 derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a cien mil Soles (S/ 100,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

[5] 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/

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

[7] Absolución a la consulta N° 39.

j) Presentar la documentación de todo el perfil solicitado en el numeral 9, los cuales deberán cumplir con los requisitos mínimos indicados en el inciso 9.1, 9.2. y 9.3 (no solicitados en los requisitos de calificación) de las especificaciones técnicas relacionado al personal para la implementación, instalación, configuración, mantenimiento preventivo, soporte técnico y seguridad gestionada.

Importante
• *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
• *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[8].*
• *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes o a través de la Agencia Virtual en Av. España N° 610, Breña, de lunes a viernes en el horario de 8:00 a 16:00 horas.

Importante
En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de compra, cuando el monto del valor estimado del ítem no supere los cien mil Soles (S/ 100,000.00).

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista, como sigue:

FORMA DE PAGO DE LA PRESTACIÓN PRINCIPAL

El pago correspondiente a la prestación principal se realizará de la siguiente forma:

1. 80% respecto de la actividad relacionada a la entrega de bienes, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.1. de 10. CONFORMIDADES" de las especificaciones técnicas.
2. 20% respecto de la actividad relacionada a la Instalación y configuración, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.2. de 10. CONFORMIDADES", de las especificaciones técnicas.

FORMA DE PAGO DE LA PRESTACIÓN ACCESORIA

Las prestaciones accesorias se pagarán conforme el siguiente detalle:

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

1. **Capacitación:** Se realizará en UNA (01) armada, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

2. **Mantenimiento Preventivo y Soporte Técnico:** Se realizará en un total de tres (03) armadas, las cuales se realizarán a razón de 1 pago al año durante el periodo de tres (03) años, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística (TICE).

3. **Seguridad Gestionada:** Se realizará un pago mensual, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

PRESTACIÓN ACCESORIA		
Componentes	**PAGOS**	**OBSERVACION**
Capacitación	100% del monto contractual de la capacitación	Previa conformidad
Mantenimiento preventivo y Soporte Técnico	40% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del primer año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del segundo año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del tercer año
Seguridad Gestionada	Mensual	Previa conformidad

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

Para proceder con el pago el Contratista deberá contar con:

Prestación Principal

- Recepción de la Guía de Ingreso de los bienes.
- Copia del Informe final de la prestación principal.
- Acta de Recepción.
- Acta de Instalación y Configuración de Equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad.
- Comprobante de Pago.
- Conformidad emitida por la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

Prestación Accesoria

- Copia del Informe de Capacitación en el cual adjunte el material digital proporcionado y una copia de los certificados entregados.
- Copia del Informe Anual de las realizadas en el mantenimiento preventivo y soporte técnico:

a) Al culminar el mantenimiento preventivo.
b) Al culminar el soporte técnico.

- Copia del Informe Mensual de las actividades realizadas de la Seguridad Gestionada.
- Comprobante de Pago
- Conformidad emitida por la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

La Entidad debe pagar las contraprestaciones pactadas a favor del Contratista dentro de los diez (10) días calendario siguiente a la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello.

Dicha documentación se debe presentar en Mesa de Partes y/o a través de la Agencia Virtual sito en Av. España N° 610, Breña de lunes a viernes en el horario de 8:00 a 16:00 horas.

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. ESPECIFICACIONES TÉCNICAS

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

ESPECIFICACIONES TÉCNICAS
ADQUISICIÓN DE HERRAMIENTA DE GESTION DE EVENTOS E INFORMACION DE SEGURIDAD

1. DENOMINACIÓN DE LA CONTRATACIÓN

ADQUISICIÓN DE HERRAMIENTA DE GESTION DE EVENTOS E INFORMACION DE SEGURIDAD.

2. FINALIDAD PÚBLICA

Proporcionar una visión global de la seguridad en la Superintendencia Nacional de Migraciones con la finalidad de detectar, responder y mitigar amenazas informáticas que afecten la disponibilidad e integridad de la información que publica y administra la Institución.

3. ANTECEDENTES

Como parte de la FASE III del Proyecto de Inversión Pública - PIP 297350 "MEJORAMIENTO DE LOS SERVICIOS MIGRATORIOS BRINDADOS EN EL LOCAL DE LA AV. ESPAÑA N° 734 DE LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES", se consideró la adquisición de una Herramienta de Gestión de Eventos e Informacion de Seguridad y así detectar de forma centralizada las amenazas informáticas y mitigarlas.

4. OBJETIVOS DE LA CONTRATACIÓN

4.1. GENERAL:

Asegurar la confidencialidad, integridad y disponibilidad de los activos, sistemas e infraestructura tecnológica de la Superintendencia Nacional de Migraciones.

4.2. ESPECIFICOS:

Adquirir e implementar una herramienta de gestión de eventos e información de seguridad con la finalidad de detectar en tiempo real y de forma centralizada las amenazas informáticas y mitigarlas.

5. ALCANCE Y DESCRIPCIÓN

El contratista debe contar y cumplir con los protocolos de distanciamiento, prevención y seguridad contra el COVID-19 en sus instalaciones según lo establecido por el Gobierno, de acuerdo a lo citado en el numeral 4.1 del Decreto Supremo N° 103-2020-EF o aquellos que tengan vigencia durante la entrega, instalación y configuración *del equipamiento de la Herramienta de Gestión de Eventos e Informacion de Seguridad*, así como durante el desarrollo de las prestaciones accesorias. Se precisa que los protocolos de distanciamiento, prevención y seguridad contra el COVID-19 deben ser cumplidos por las personas a quienes delegue las actividades contenidas en el presente término de referencia.

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

[1]La presente adquisición se ha divido en prestación principal y prestaciones accesorias, por lo que se presentará para la firma del contrato una estructura de costos diferenciada para dichas prestaciones..

El postor debe presentar en su oferta, una matriz de cumplimiento punto por punto, para lo cual añadirá una columna en cada característica solicitada donde debe colocar el número de folio que evidencie el cumplimiento de lo solicitado a través de referencias a datasheets o manuales o links o imágenes los cuales se deben adjuntar.

[2]Todos los componentes, partes y/o piezas, cables, accesorios, deben ser nuevos y de primer uso.

[3]El total del equipamiento que proporcione para dar cumplimiento a las características solicitadas en la Matriz de cumplimiento punto por punto, debe estar vigente tecnológicamente y debe ser el último modelo lanzado por el fabricante al mercado, lo cual debe ser respaldado con una carta del fabricante (Debe adjuntar la lista de equipos indicando marca y modelo)

El contratista debe proporcionar los equipos, accesorios, licencias, suscripciones o cualquier componente de hardware o software que permita que su solución ofertada cumpla con lo siguiente:

	CARACTERISTICAS TÉCNICAS MÍNIMAS
1	La solución debe proveer debe tener administración personalizable y basada en web: Monitoreo de Seguridad, Investigación basada en metadatos de eventos de seguridad, Reportes para Cumplimiento normativo.
2	La solución SIEM con la que se aprovisione el servicio deberá contar con las siguientes capas respecto de la arquitectura y diseño: a) Colección. b) Administración de Logs (Log Management) c) Administración de Eventos (Event Management) d) Correlación de eventos e) Alarmas f) Manejo de Incidentes y casos g) Reportes
3	Lo solicitado para el componente SIEM son appliance de propósito específico los cuales deben ser de la marca de la solución ofertada. No se aceptará soluciones virtualizadas en un servidor y sobre un hypervisor.
4[4]	El componente SIEM de la solución debe estar basado en una base de datos relacional (RDBM) o no relacional o repositorio propietario del fabricante (BIG DATA) que garantice la gestión de su información y el manejo de las bitácoras/logs.

[1] **Absolución de la Consulta N° 39, formulada por SECURESOFT CORPORATION S.A.C:** Dicha estructura de costos diferenciada se presentará para la firma del contrato.

[2] **Absolución de la Observación N° 11, formulada por TELEFONICA DEL PERU S.A.A.:** Se retirará el término "etc".

[3] **Absolución de la Consulta N° 59, formulada por SECURESOFT CORPORATION S.A.C:** Se actualizará quedando redactado de la siguiente manera: El total del equipamiento que proporcione para dar cumplimiento a las características solicitadas en la Matriz de cumplimiento punto por punto, debe estar vigente tecnológicamente y debe ser el último modelo lanzado por el fabricante al mercado, lo cual debe ser respaldado con una carta del fabricante (Debe adjuntar la lista de equipos indicando marca y modelo).

[4] **Absolución de las Consultas N° 20 y N° 21, formulada por BEKER PERU S.A.C..:** Quedará redactado de la siguiente manera: El componente SIEM de la solución debe estar basado en una base de datos

5	La integridad de la base de datos o repositorio debe tener protección de los datos a través de cifrado o protegido por HASH
6	La solución SIEM debe estar basada en una base de datos de acceso general (publico) o en la cual sea posible su acceso por aplicaciones de terceros para reporteo externo y no en bases de datos propietarias cerradas que impiden el acceso a los datos forenses (logs/paquetes, etc).
7	Debe contar con un modelo de manejo de datos dentro de la base el cual sea modificable por configuración para permitir ajustar utilización (espacio en storage) de la capa de eventos, manejo de logs y detalles específicos a almacenar de manera granular, así como poder definir qué tipo de información "tirar" y cual almacenar por un tiempo específico.
8	Debe permitir acceder a los logs originales (raw log data), siempre que así se desee, además de contar con la información previamente interpretada por la solución de inteligencia del SIEM (Eventos, Alarmas e Incidentes)
9	Debe contar con una consola administrativa misma que puede tener accesos vía Web (HTTPS).
10	Dicha consola debe poder visualizarse en dispositivos móviles en sistemas operativos como Android e IOS (Deberá estar habilitada para "touch")
11	La solución debe contar con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada.
12[5]	Debe mantener cifrado en los componentes de autenticación y en las capas de transporte de datos, opcionalmente este cifrado podrá ser desactivado en algunos componentes para proveer funcionalidades de agilización de transferencias de datos.
13	Debe estar basado en una plataforma endurecida (Hardened) de sistema operativo Windows o Linux.
14[6]	Se deber poder aplicar parches al sistema operativo de manera discrecional conforme recomendaciones del fabricante y/o tercero que personalizó el sistema operativo sin impactar el rendimiento y presentación de la aplicación
15[7]	La solución SIEM con la que se aprovisione el servicio deberá estar dentro del cuadrante de líderes de Gartner de 2020 en Security Information and Event Management. (opcional)
16	Debe soportar 2500 eventos por segundo y tener la capacidad de incrementar dicho valor en un 30% sin necesidad de agregar, cambiar o actualizar hardware.
17	Los agentes deberán estar certificados por el fabricante además de disponibles para plataformas: Windows Server 2008 (64 Bits), Windows Server 2008 R2 (64 Bits), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 7 (64 Bits), Windows 8, Windows 10, Linux RedHat Enterprise
18[8]	La solución debe contar con agentes o un módulo independiente que permita convertirse o implementar un colector de eventos de otras plataformas. Se precisa que el colector de eventos

relacional (RDBM) o no relacional o repositorio propietario del fabricante (BIG DATA) que garantice la gestión de su información y el manejo de las bitácoras/logs.

[5] **Absolución de las Consultas N° 25 y N° 26 formuladas por BEKER PERU S.A.C., N° 127 formulada por BIGSECURE S.A.C..:** Quedará redactado de la siguiente manera: "Debe mantener cifrado en los componentes de autenticación y en las capas de transporte de datos, opcionalmente este cifrado podrá ser desactivado en algunos componentes para proveer funcionalidades de agilización de transferencias de datos."

[6] **Absolución de la Consulta N° 29 formulada por BEKER PERU S.A.C..:** Quedará redactado de la siguiente manera: "Se deber poder aplicar parches al sistema operativo de manera discrecional conforme recomendaciones del fabricante y/o tercero que personalizó el sistema operativo sin impactar el rendimiento y presentación de la aplicación."

[7] **Absolución de las Observaciones N° 19 formulada por TELEFONICA DEL PERU S.A.A., N°31 formuladas por BEKER PERU S.A.C. y Absolución a la consulta N° 30 formulada por BEKER PERU S.A.C.:** Se indicará que este requerimiento es opcional.

[8] **Absolución de las Consultas N° 47 y N° 48 formulada por SECURESOFT CORPORATION S.A.C:** Se actualizará agregando lo siguiente: Se precisa que el colector de eventos puede ser virtualizado solo en el caso que sea requerido en una zona de colección remota [La Entidad brindará un equipo físico o

	puede ser virtualizado solo en el caso que sea requerido en una zona de colección remota (La Entidad brindara un equipo físico o virtual, siempre que este no requiera recursos mayores a 2 core de CPU, 4 GB de RAM y 100 GB de disco duro).
19	Los agentes o módulos de la solución deben contar con la posibilidad de separar "relay hosts" (Servidores de Syslog que envían múltiples cadenas de logs detrás de ellos) y manifestarlos de manera independiente para realizar correlación correcta.
20	Los agentes o módulos de la solución deben contar con la posibilidad de convertirse en colectores de flujos (Netflow o Jflow o sFlow o IPFIX), SNMP traps.
21	Los agentes o la solución deben tener la posibilidad de realizar Host Activity Monitoring dentro de la solución (Al menos para servidores Windows)
22[9]	Los agentes o la solución deben tener la posibilidad de realizar Monitoreo en Tiempo Real, o modo batch y cuando aplique permitir políticas de Monitoreo de Registro de Windows. Se precisa que lo requerido en este punto, es que la solución a través de los agentes soporte y/o cumpla esta característica, sin embargo, no forma para del presente requerimiento la provisión o instalación de dichos agentes.
23[10]	De manera adicional los agentes o la solución deberán contar con la posibilidad de agendar los periodos de monitoreo de carpetas y archivos de logs con fines de poder realizar colección en horarios no productivos y su reporteo a infraestructuras de manejo de logs en horarios específicos con fines de evitar congestionamientos específicos con infraestructuras de comunicaciones para locaciones remotas. Se aceptará que en los agentes o la solución se pueda configurar que eventos (en función del dispositivo que los genera y su criticidad para la institución) deben ser enviados en línea y que eventos puedan ser agendados para enviarse en otro horario.
24	Los agentes, además de los puntos antes mencionados, deberán permitir la colección de mensajes vía API, Sockets, FTP, SSH, SCP o en general cualquier mecanismo disponible mediante la tecnología de BEATS.
25	La solución SIEM, debe manejar una capa de información viva (live data) para búsquedas avanzadas y detalladas hasta por 120 días.
26	La solución SIEM, debe contar con una capa de información en reposo (cold data) siempre permitiendo utilizar datos viejos archivados fuera de la infraestructura en reportes e investigaciones forenses inclusive hasta 6 meses.
27	La solución SIEM, debe acoplarse mediante configuración a utilizar las soluciones de STORAGE que la institución tenga o adquiera en el futuro (NAS/SAN), sin necesidad de utilizar soluciones de almacenamiento propietarias. Lo anterior no debe representar ningún costo para la Entidad.
28	Los logs archivados deberán tener la funcionalidad de almacenarse y deberán tener la tipificación básica de evidencia legal bajo el concepto (digital chain of custody) todo ello por medio de la no alteración y la custodia de los logs originales.
29	La solución deberá realizar funciones normalización y mediación en su capa de administración de logs (log management) no en su capa de colección para aminorar el impacto a los equipos que realizan las funciones de colección.

virtual, siempre que este no requiera recursos mayores a 2 core de CPU, 4 GB de RAM y 100 GB de disco duro).

[9] **Absolución de la Consulta N° 66 formulada por BEKER PERU S.A.C..: Se agregará lo siguiente:** Se precisa que lo requerido en este punto, es que la solución a través de los agentes soporte y/o cumpla esta característica, sin embargo, no forma para del presente requerimiento la provisión o instalación de dichos agentes.

[10] **Absolución de la Consulta N° 67 formulada por BEKER PERU S.A.C..: Se agregará lo siguiente:** Se aceptará que en los agentes o la solución se pueda configurar que eventos (en función del dispositivo que los genera y su criticidad para la institución) deben ser enviados en línea y que eventos puedan ser agendados para enviarse en otro horario.

30	Se deberán poder separar archivados por entidad e infraestructura con fines de poder gestionar backups de esos archivados de manera separada sin impactar los backups generales de la plataforma, lo anterior tiene el fin de que la solución muestre un arreglo de multi tenencia (Multi-Tenant) donde las bitácoras archivadas se puedan separar de manera general por cliente, edificio o grupo, dependiendo la configuración que la Entidad requiera, sin tener que trabajar con la plataforma completa.
31[11]	El sistema de administración de Bitácoras deberá permitir configurar la utilización de memoria y CPU para su procesamiento (opcional)
32[12]	Cuando la cantidad de logs recibida sobrepase la capacidad licenciada de logs, la solución NO deberá "tirar/borrar" los logs y así asegurar su procesamiento.
33	La solución deberá permitir realizar distribución de los logs ya procesados (por el log-manager) a una solución de un tercero para soluciones de maximización de componentes. (Ejemplo: Enviar los logs a otro manejador de eventos, pero previamente procesados)
34	El sistema de administración de logs deberá permitir la utilización de certificados digitales específicos TLS.
35[13]	Debe contar con un framework o método sencillo para poder integrar nuevos dispositivos no detectados conforme necesidades futuras de la institución en cuestión de normalización de bitácoras. Este framework deberá permitir la adecuación de expresiones regulares básicas (regex) o plantillas XML para adecuar las reglas de "parsing" cortado y normalización.
36	El sistema de administración de logs deberá contar con la posibilidad de configurar de manera discrecional, que es un evento y que no, de todos los logs que se reciben, con fines de maximizar las capacidades de análisis de información importante e información intrascendente.
37	El sistema de administración de logs deberá contar con la posibilidad de traducir de manera automatizada y en tiempo real PAISES en vez de mostrar solo direcciones IP para los eventos que sean reenviados al sistema de administración de eventos.
38	La solución SIEM debe brindar auto-clasificación de los datos capturados en modo estructurado con fines de brindar funcionalidades de búsquedas estructuradas (structured search), pero también brindar funcionalidades de búsqueda no estructurada, esto quiere decir que el sistema de inteligencia podrá ser consultado en función de estructuras específicas de datos conocidas pero también deberá permitir consultar datos sin conocer su estructura (unstructured search), lo anterior deberá estar presente en un producto único sin necesidad de duplicar la información.
39	El sistema de administración de eventos deberá contar con la posibilidad de brindar una consola general para la consulta de la información en tiempo real, para realizar investigaciones forenses al pasado y tener la capacidad de mostrar una visión de tendencias hacia el futuro sobre los distintos eventos que se presenten en la plataforma.
40	Debe permitir diseñar modelos de cálculo de riesgo basado en formulas específicas dictaminadas por la Entidad a fin de tomar decisiones acordes con la tipificación específica de la amenaza en cuestión, tomando como base la información colectadas por los eventos basados en su criticidad y editar el valor de riesgo que por defecto tiene dicho evento.
41	Las consolas de administración en conjunto con el sistema de administración de eventos deberán permitir la visión y búsqueda de más de 60 campos de metadatos normalizados para auto filtrado automatizado en donde puedan seleccionarse condicionales específicas.
42	La consola de administración de la solución de administración de eventos y logs deberá permitir generar Layouts o dashboards específicos por persona e infraestructura que es la que analiza los datos, esto quiere decir que la vista general de la solución debe permitir configuraciones específicas

[11] **Absolución de las Consultas N° 49 formulada por SECURESOFT CORPORATION S.A.C y N° 70 formulada por BEKER PERU S.A.C..:** Se precisa que esta característica será opcional

[12] **Absolución de la Consulta N° 71 formulada por BEKER PERU S.A.C..:** Quedará redactado de la siguiente manera: Cuando la cantidad de logs recibida sobrepase la capacidad licenciada de logs, la solución NO deberá "tirar/borrar" los logs y así asegurar su procesamiento.

[13] **Absolución de la Consulta N° 72 formulada por BEKER PERU S.A.C..:** Se agregará el término "plantillas XML"

MIGRACIONES PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

	por analista y perfil de búsqueda sin necesidad de re-configurar todo cada vez que se autentica a la misma.
43	La consola de administración debe contar con la posibilidad de mostrar información realmente en tiempo real y no en procesamiento batch, esto quiere decir que la información que esta cambiando en un aplicativo, sistema operativo o firewall debe ser virtualmente posible veria inmediatamente reflejada en la consola de administración sin esperar tiempos considerables a realizar esta tarea.
44	La consola de administración deberá permitir ordenar "sortear" la información conforme necesidades específicas en tiempo real sin necesidad de la gestión de consultas o querys complicados.
45	La consola de administración deberá contar con la posibilidad de agrupar eventos parecidos con fines de verlos de una manera más sencilla y no repetirlos, además de contar con la posibilidad de generar gráficos específicos de tiempo inicial y tiempo final en la que ocurrieron los eventos.
46	La consola de administración deberá contar con vistas en tiempo real como: a) Estadísticas de eventos comunes. b) Estadísticas de eventos con IP origen. c) Estadísticas de eventos con Host origen. d) Estadísticas de eventos con IP destino (equipo que han sido impactados). e) Estadísticas de eventos con Host destino (equipo que han sido impactados). f) Estadísticas de aplicaciones impactadas. g) Estadísticas de fuente de logs específicos. h) Logs por semana, día y hora. i) Logs por tiempo y dirección.
47[14]	La consola de administración debe contar con la posibilidad de hacer clic sobre algunos objetos y obtener información de que simboliza en una gráfica, debe contar con un nivel máximo y mínimo de abstracción (drag-in, drag-out), de igual manera los componentes del dashboard deben de poder ser "detacheables" para manejar soluciones de video wall.
48	La consola de administración deberá contar con la posibilidad de utilizar listas de objetos, cosas, direcciones IP, países, etc, estas listas deberán poder compartirse entre usuarios y auto administrarse dentro de la solución.
49	57) Deberá promover una integración nativa con información de inteligencia de amenazas (Threat Intelligence) de fuentes OpenSource con un formato específico incluyendo STIX/TAXII.
50	Deberá proporcionar un acceso rápido a información contextualizada dependiendo del tipo de dato que se haya seleccionado, por ejemplo, en caso de seleccionar una dirección IP, deberá proporcionar acciones de contexto para buscar esa IP en fuentes de inteligencia de direccionamiento o en buscadores de propósito general como Google.
51	Las funcionalidades de correlación y normalización de datos, deberá realizarse en tiempo real de manera comprobable, evidenciando el modelo completo de normalización y tratamiento de los datos, creación de reglas y normalización de tiempo, permitiendo correlacionar datos "fuera de tiempo" incluso.
52	El sistema deberá contar con una funcionalidad de actualización (automática o manual, dependiendo sea la necesidad) de inteligencia de parte del fabricante que por lo menos actualice formatos nuevos detectados de bitácoras, eventos nuevos y riesgosos, nuevas políticas de alertamiento, modificaciones en estándares.
53	La consola de administración deberá proveer la funcionalidad de agrupar de manera completa dispositivos, hosts, redes y activos específicos para poder asignar locaciones, dirección de conectividad (inside, outside, local, etc) así como el nivel de riesgo de cada activo el cual estará ligado a la cantidad de eventos e importancia que cada uno de ellos refiera de manera aislada.
54	Además de separar completamente la información de estas entidades internamente para que se habilite el concepto de "multi-tenant" SIEM.

[14] **Absolución de la Consulta N° 75 formulada por BEKER PERU S.A.C.: Se cambiará el término a "algunos objetos"**

55	El sistema de administración de eventos deberá contar con la posibilidad de correlacionar de manera básica eventos por contenido de login, IP, histórico en tiempo.
56[15]	Quedará redactado de la siguiente manera: El sistema de correlación de eventos avanzado deberá contar con más de 600 reglas de correlación o políticas pre-definidas de detección de patrones.
57[16]	El sistema de correlación de eventos avanzado deberá ser manejado de manera completa por medio de wizards gráficos (drag and drop) o a través de opciones y menús que proporcione la WebUI, sin la necesidad de conocer lenguajes de programación para la gestión de políticas nuevas.
58	El sistema de correlación de eventos avanzado deberá nutrirse no solo de información de eventos (limited subset) sino de flujos de datos (netflow o jflow o sflow o ipfix), logs nativos, etc para proveer la máxima capacidad de abstracción posible para la detección de amenazas complejas y advanced persistent threats.
59	El sistema de correlación de eventos avanzado deberá permitir activar y desactivar las políticas durante un tiempo específico con fines de monitorear la utilización de CPU donde se están realizando estas comprobaciones a su vez la utilización de memoria RAM que es gastado en cada función de correlación avanzada.
60[17]	El sistema de correlación de eventos deberá contar con la posibilidad de agrupar las políticas que se ejecutan en tiempo real y ordenarlas para evitar errores de obtención de información una vez que se cumplen X o Y factores. (opcional)
61	El sistema deberá integrarse de manera nativa con Microsoft Active Directory, con fines de extracción de la base total de usuarios y grupos para realizar correlación multidimensional y jerárquica.
62	El sistema deberá proporcionar herramientas para integrarse con cualquier solución de gestión de identidades para la obtención confiable de usuarios de la institución.
63	El sistema deberá permitir como mínimo a 4 administradores y analistas, acceder a información independiente de manera centralizada y recurrente (al mismo tiempo).
64	El sistema deberá contar con una base de datos local de autenticaciones para manejar usuarios en caso de no desear alinearlo a la infraestructura de Microsoft Active Directory de la institución.
65	El sistema deberá permitir desactivar de manera temporal cuentas sin necesidad de borrar toda la información de autenticación a la plataforma una vez que un empleado se le deniegue el acceso a dicha plataforma.
66	El sistema deberá permitir manejar grupos y roles por grupo para poder manipular con mayor sencillez a los usuarios.
67	El sistema deberá contar con la posibilidad de limitar el nivel de acceso conforme la credencial autenticada y esto concordar con el perfil asignado a cada empleado sobre el tipo de información a la cual se tiene acceso (fuentes de logs, configuraciones, etc).
68	El sistema de administración de eventos deberá permitir configurar que datos deben ser compresos y cuales no, en detalle de la base de datos de eventos al igual cual será el valor de compresión de los índices.
69	El sistema de administración de eventos deberá manejar índices pre-calculados para agilizar las investigaciones.
70	La consola de administración debe brindarse por medio de web, no deberá utilizar flash o Java (tecnologías que brindan un riesgo completo y que incluso el soporte por default de los principales navegadores ha sido removido por cuestión de seguridad), deberá plasmarse la tecnología que cuenta ya que se busca que esta pueda ser visualizada en tablets, celulares y computadoras sin tener que instalar plugins ni aplicaciones extras al navegador común.

[15] **Absolución de la Consulta N° 77 formulada por BEKER PERU S.A.C..:** Quedará redactado de la siguiente manera: El sistema de correlación de eventos avanzado deberá contar con más de 600 reglas de correlación o políticas pre-definidas de detección de patrones

[16] **Absolución de la Consulta N° 78 formulada por BEKER PERU S.A.C..:** Se agregará: "o a través de opciones y menús que proporcione la WebUI"

[17] **Absolución de la Consulta N° 79 formulada por BEKER PERU S.A.C..:** Se precisará que esta característica es opcional.

MIGRACIONES PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

71	La consola de administración debe permitir contenidos de visualización tales como mapas de conectividad (connection maps/contextualization maps), indicadores de compromiso (IOC) y configuraciones completas por el cliente para visualizar cualquier tipo de dato que se encuentre procesado por la solución.
72	La plataforma deberá contar con la posibilidad de construir interfaces de propósito específico con visualizaciones específicas en tableros de ciber inteligencia con el fin de brindar visibilidad de modo general y particular de acuerdo a los requerimientos de la Entidad.
73	El sistema de manejo de alarmas debera proveer las funcionalidades de alertar en función de observar consideraciones, patrones y condicionales específicas en cualquiera de las capas atrás mencionadas: a) Colección. b) Administración de Logs (Log Management). c) Administración de Eventos (Event Management). d) Correlación de Eventos
74	Las alarmas deberán de manejarse como datos aislados de incidente promoviendo las funcionalidades de dar seguimiento oportuno por medio de alertas vía correo electrónico, ejecución de programas específicos o escritura a archivos planos para procesamiento futuro con otras herramientas.
75[18]	El sistema de alarmas debera integrarse de manera sencilla con Remedy, OTRS u otras herramientas, por medio de correo electrónico o archivo plano o SNMP o API o REST API, con un layout específico para que oportunamente se pueda dar seguimiento a los casos detectados.
76	El sistema de alarmas deberá contar con un sub-sistema de remediación, para realizar actividades propias de remediación.
77[19]	El sistema de remediación deberá contar con un framework basado en plugins o scripts para bloquear cuentas, inyectar reglas en los firewalls, bloquear puertos en switches, apagar equipos de cómputo.
78	El sistema de remediación deberá proporcionar Playbooks con acciones o procedimientos a seguir que puedan ser asignados según las necesidades de cada departamento de la institución.
79	El fabricante deberá proporcionar plugins por lo menos para las siguientes actividades: a) Deshabilitar cuenta en directorio activo. b) Terminar proceso en Windows y *nix de manera remota. c) Manejo de servicios (Up, Down, Monitoring). d) Adherir objetos componentes a lista (IP, Dominio, Cosa). e) Deshabilitar cuenta local en equipo Windows. f) Inyectar políticas a Palo Alto, Checkpoint, ASA.
80	El sistema de alarmas deberá proveer funcionalidades para notificar alarmas y que puedan segregarse en el panel del dashboard principal a placer (layouts)
81	El sistema de alarmas y manejo de incidentes debe permitir asignar el estatus a una alarma dentro de la misma herramienta con fines de que se mantenga comunicación interna entre el personal que ocupa la herramienta para saber si una alarma ha sido escalada, se está trabajando en ella o se trataba de un falso positivo, ha sido resuelta, se continuara monitoreando o no ha sido ni será resuelta además de permitir al usuario asignar comentarios a cada momento.
82	El sistema de alarmas y manejo de incidentes permitirá conocer cuál es el histórico (quien la tocó, quien la abrió, quien la cerró, quien respondió a ella, cuando) de una alarma con fines de su futura explotación y auditoria.

[18] **Absolución de la Consulta N° 135 formulada por BIGSECURE S.A.C.: Se agregará la frase "o API o REST API"**

[19] **Absolución de la Consulta N° 82 formulada por BEKER PERU S.A.C.: Se agregará la palabra "o scripts"**

83[20]	El sistema de alarmas contará con un compendio específico y un set de condiciones para declarar cosas que salen de cumplimiento, por ejemplo, se debe contar con alarmas preestablecidas de rompimiento de estándares generales como PCI-DSS, ISO 27001 o ISO 27002, SOX(opcional).
84	La solución SIEM, debe proporcionar un proceso completo desde la captura de las bitácoras, indicadores y demás datos de maquina (machine data) hasta la gestión y documentación del incidente visualizado, donde deberá proporcionar un visor de incidentes.
85	La herramienta de manejo de casos (Case Management) deberá poder interactuar con herramientas de manejo de tickets del SOC con fines de poder realizar interacción bidireccional de las evidencias (logs, screenshots, imágenes forenses de disco, capturas de paquetes).
86	La herramienta de manejo de casos (Case Management) deberá promover un escenario jerárquico de dictaminación de incidentes en el cual se pueda asignar riesgo, colaboradores, analistas y staff que no debe de visualizar un dato específico. Lógicamente la herramienta de manejo de casos debe interactuar con el sistema de remediación para por medio de flujos de trabajo (workflows) poder responder a un incidente.
87	La solución SIEM deberá contar con la posibilidad de generar reportes avanzados de los siguientes estándares con la adecuación completa a requerimientos de auditoria en caso de existir: a) HIPAA. b) ISO 27001 o ISO 27002. c) PCI-DSS . d) SOX
88	La solución SIEM deberá contar con reportes de estándares y plantillas modificables por el usuario de categorías como las siguientes: a) Tops atacantes b) Vulnerabilidades c) Amenazas d) Alarmas detonadas e) Violaciones de cumplimiento f) Fallos operativos g) Violaciones de auditoria h) Reportes ejecutivos i) Detalles de logs (volumen, detalle, capacidad) j) Estadísticas de los componentes de la solución (Log Management, Event Management) k) Resúmenes y templates específicos
89	La solución SIEM, debe mostrar los reportes en pantalla antes de solicitar cualquier exportación a formatos externos.
90	La solución SIEM, debe guardar un registro completo de que reportes que se producen y almacenar un cache para acceso más tarde sin necesidad de ejecutar nuevamente el reporte lo cual reduce el tiempo de entrega de los mismos. Asimismo, deben exportarse a los siguientes formatos: a) CSV b) PDF
91	Los reportes deben de contar con un análisis discrecional de privilegios dentro de la organización para solo permitir que las personas que puedan verlo sean las únicas que tienen acceso a ellos.
92	Los reportes deberán estar visibles en la consola Web por un mínimo de 7 días y un máximo de 30 y su acceso debe ser discrecional al rol que accede a la consola.
93	El licenciamiento debe ser basado en cantidad de Eventos por Segundo y NO en la cantidad de dispositivos que se deban integrar.
94	La solución debe poder integrarse con soluciones de gestión de vulnerabilidades.
95	La solución debe tener la capacidad de aprender los patrones de comportamiento de los procesos de monitoreo, a fin de mejorar los indicadores de detección temprana de las amenazas cibernéticas.

[20] **Absolución de la Consulta N° 85 formulada por BEKER PERU S.A.C.: Se indicará que SOX es opcional.**

96	La solución debe analizar el tráfico IPv4 e IPv6.
97	La solución debe tener documentada la lista de integraciones nativas soportadas.

Adicionalmente, el contratista debe proporcionar e instalar lo siguiente:

A) *Una solución de Video Wall que consista de lo siguiente:*

Estructura para Video Wall:

Características	Descripción
Soporte	Estructura para arreglo de Video Wall de 2x2 para pantallas de hasta 40" hasta 60"
Tipo de Estructura	Piso a Techo fabricada en acero SAE 10.10
Pintura	Epóxica negra texturizado

Para los racks se deberá considerar lo siguiente:

Características	Descripción
Cantidad	04
Tipo	Pop – Out
Pintura	Electrostática
Configuraciones	Montaje de liberación rápida
Capacidad	Soporte para pantallas de hasta 70 Kg.

[21] *Pantallas de Video Wall – Cantidad 04*

Las pantallas deberán ser específicas para video Wall, no se aceptarán televisores o similares, las características mínimas para las pantallas deberán ser:

Característica	Descripción
Tamaño	55" o superior
Alimentación	100-240 V @ 60Hz
Resolución	1920x1080 FHD

[21] **Absolución de la Observación N° 91 formulada por BEKER PERU S.A.C., Absolución de las consultas N° 114 formulada por GRUPO ELECTRODATA S.A.C. y N° 115 formulada por GRUPO ELECTRODATA S.A.C.:** La referencia a las pantallas de videowall, quedarán de la siguiente manera: Característica/Descripción: Tamaño 55" o superior, Alimentación 100-240 V @ 60Hz, Resolución 1920x1080 FHD, Panel LED o similar, Distancia de bisel a bisel 3.7 mm (máximo), Conectividad de entrada DP 1.2 / HDMI, Salida DP 1.2, Red Ethernet RJ45, Calibración Automática. Al unirse las pantallas deben formar un videowall de 4K.

Panel	LED o similar
Distancia de bisel a bisel	3.7 mm (máximo)
Conectividad de entrada	DP 1.2 / HDMI
Salida	DP 1.2
Red	Ethernet RJ45
Calibración	Automática.

Al unirse las pantallas deben formar un Videowall de 4K.

[22]En caso que la consola de gestión de videowall, sea un equipo de propósito específico y de la marca del videowall debe cumplir con lo indicado para el "Software Controlador". En caso que la consola no sea un equipo de propósito específico de la marca, debe cumplir con lo indicado para el Software Controlador y para el "Servidor para Controlador de Videowall".

Software controlador (Cantidad 01)

Característica	Descripción
Tipo de funcionamiento	Solución tipo AV-over-IP (transmisión de video sobre red)
Tipo de solución	Instalada en servidor local
Gestión[23]	Por medio de navegador web (https) sin necesidad de contar con agente o cliente instalado en equipo del administrador
	Control de acceso basado en roles con permisos multinivel
	Permita ejecutar backups en horarios y recuperar la plataforma en caso sea necesario
	Administración remota del videowall (desde una ubicación externa)
Operación	Por medio de navegador web sin necesidad de contar con agente o cliente instalado en el equipo del operador
	Permitir mostrar la pantalla del operador sin contar con agente o cliente instalado en el equipo operador
	Permitir agregar contenidos sin límite en las pantallas
	Creación de horario de visualizaciones de contenidos
	Permitir superponer un contenido sin necesidad de modificar el diseño de los contenidos (Picture in Picture – PIP)
	Capacidad de interactuar con el contenido de manera remota, tanto en teclado como ratón (KVM remoto)
Contenidos soportados	RTSP Escritorio del administrador/Operador Web (HTML5) Aplicaciones de escritorio Imágenes Videos (MP4, soporte de encoder H264 y H265) VNC

[22] **Absolución de la Consulta N° 55 formulada por SECURESOFT CORPORATION S.A.C:** Se agregará lo siguiente: En caso que la consola de gestión de videowall, sea un equipo de propósito específico y de la marca del videowall debe cumplir con lo indicado para el "Software Controlador". En caso que la consola no sea un equipo de propósito específico de la marca, debe cumplir con lo indicado para el Software Controlador y para el "Servidor para Controlador de Videowall".

[23] **Absolución de la Consulta N° 121 formulada por GRUPO ELECTRODATA S.A.C.:** Por medio de navegador web (https) sin necesidad de contar con agente o cliente instalado en equipo del administrado

	RDP

Servidor para Controlador de Videowall:

El servidor debe ser rackeable y cumplir con las características solicitadas por el fabricante para su correcta ejecución, sin embargo, deberá al menos contar con las siguientes características mínimas:

- De Procesador de 08 núcleos (16 hilos).
- Memoria de 64 GB.
- 1 TB de almacenamiento SSD.
- Para el procesamiento correcto del contenido, se solicita que cuente con al menos una tarjeta de video RTX 2080 o superior
- Tarjeta de red: deberá contar con al menos 02 tarjetas de red.

Instalación, configuración y capacitación de Videowall

Instalación física de la estructura para el videowall, la cual debe considerar:

- Anclaje de estructura videowall hacia el lugar designado para la instalación.
- Anclaje de los racks para videowall a la estructura.
- Instalación de los monitores en los racks para videowall
- Para la entrega, el contratista debe entregar los monitores alineados de acuerdo con las mejores prácticas del fabricante.
- Instalar y rackear el servidor de Videowall en el centro de datos o cuarto de comunicaciones, Migraciones dará las facilidades técnicas para la instalación de dicho servidor, (espacio en rack, energía y punto de datos).
- El proveedor deberá considerar el cableado energético, datos, video y cualquier otro cableado necesario para el funcionamiento de la plataforma, Migraciones dará las facilidades técnicas para la instalación de dicho cableado, ejemplo: caja de distribución eléctrica.
- Calibración de la pantalla de acuerdo con el ambiente.
- Postor deberá considerar los reproductores o clientes para la instalación del videowall.
- Cada pantalla deberá ser única, no se aceptará arreglos en modo cascada.

El contratista debe realizar el cableado de red y eléctrico de al menos 50 metros hasta el cuarto de comunicaciones más cercano, además debe independizar el circuito eléctrico al que irán conectadas los puntos eléctricos que instale y a los que se conectaran los equipos y/o dispositivos que formen parte de la solución de video wall (debe considerar la provisión del cableado, las canaletas, interruptores ,tablero, tomas, etc.), así como brindarles protección eléctrica y autonomía a través de UPS o baterías rackeables, por al menos 30 minutos, considerando en esta autonomía una carga adicional de 2000 Watts (Lo anterior no incluye al servidor, el cual será instalado en el centro de datos).

[24] *Se precisa que el tablero eléctrico de donde se sacará el circuito de alimentación para el videowall debe colocarlo el contratista, asimismo este tablero eléctrico debe conectarse al tablero eléctrico general que esta aproximadamente a 50 metros (Debe considerar que el tablero eléctrico general está en el primer piso y el tablero que debe colocar está en el piso 6)*

Adicionalmente debe considerar la instalación de 7 puntos de red y 7 puntos eléctricos hacia el ambiente donde instalará el video Wall los cuales se deben conectar al mismo circuito eléctrico indicado en el párrafo anterior.

Capacitación en el uso de la plataforma video wall que incluye:

- Administración de la plataforma
- Configuración de contenidos
- Compartir pantalla.
- Demostración de funcionamiento de interacción.

B) El contratista debe proporcionar e instalar un (1) dispositivo de control de acceso biométrico sin contacto (incluido su punto de red de 60 m) así como su cerradura y todo lo necesario para su instalación en una puerta de una de las oficinas en la Sede Central. Como mínimo este dispositivo de control de acceso debe cumplir con: 3.9 pulgadas touch screen, 2 MP wide-angle lente dual, exactitud de reconocimiento facial >= 99%, reconocimiento facial < 0.2 s/usuario, distancia de reconocimiento [0.3m, 1.5m], face anti-spoofing soporte para un mínimo de 6 estados (check in, check out, break in, break out, overtime in, overtime out), debe tener un seguro de tal forma que evite que la puerta se abra cuando el control de acceso de dañado (via RS-485) y considerar su apertura en caso no se tenga energía eléctrica.

5.1. PRESTACION PRINCIPAL

Debe trabajarse bajo el enfoque de gestión de proyectos, entregándose los planes de gestión del proyecto conforme a las áreas de conocimiento.

5.1.1. ENTREGA, INSTALACION Y CONFIGURACIÓN.

El contratista debe realizar la entrega de la solución ofertada (biens, que da cumplimiento a lo solicitado en el presente documento, en el almacén ubicado en la Sede Central de la Superintendencia Nacional de Migraciones con sitio en Av. España 734- Breña, previa coordinación con la Oficina General de Tecnologías de Información, Comunicación y Estadística (TICE).

[24] **Absolución de las Consultas N° 97 formulada por BEKER PERU S.A.C. y N° 108 formulada por TELEFONICA DEL PERU S.A.A:** Se agregará: Se precisa que el tablero eléctrico de donde se sacará el circuito de alimentación para el videowall debe colocarlo el contratista, asimismo este tablero eléctrico debe conectarse al tablero eléctrico general que esta aproximadamente a 50 metros (Debe considerar que el tablero eléctrico general está en el primer piso y el tablero que debe colocar está en el piso 6)

El contratista debe realizar la instalación de los equipos y/o componentes en el Centro de Datos de las Superintendencia Nacional de Migraciones, ubicado en la Av. España N° 734 – Distrito Breña, para lo cual debe rackearlos apropiadamente en los gabinetes de comunicaciones que se le indicaran; debe proporcionar los cables de poder (no se aceptarán adaptadores para conectar los cables de poder a las regletas existentes), así como los patch cord certificados en al menos categoría 6, que se necesiten para conectar los equipos provistos a los switches propiedad de la Institución (debe cumplir con las normas de cableado estructurado incluida la TIA/EIA – 606).

La prestación principal finaliza cuando se firme el "*Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*".

5.1.2. GARANTÍA

La Garantía solicitada aplica para todo el hardware y software proporcionado y las funcionalidades que conforman la presente adquisición, contra defectos de diseño y/o fabricación, averías o fallas de funcionamiento.

El contratista entiende y acepta que el plazo de garantía mínima por todo el equipamiento y sus funcionalidades es de tres (03) años, la cual debe iniciar a partir del día siguiente de la firma del "*Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*" que será firmado entre el responsable del proyecto por parte de la Oficina de Tecnologías de Información, Comunicación y Estadística (TICE) y el Jefe de Proyecto del contratista.

Los trabajos derivados de la aplicación de la garantía no tendrán ningún costo para la Superintendencia Nacional de Migraciones.

5.2. PRESTACIONES ACCESORIAS

Se dan por el plazo de la garantía (03 años a partir del día siguiente de la firma del "*Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*").

5.2.1. MANTENIMIENTO PREVENTIVO Y SOPORTE TÈCNICO

5.2.1.1. El servicio de mantenimiento preventivo debe realizarse para todo el equipamiento ofertado, UNA (01) vez al año durante el periodo de vigencia de la garantía, las fechas de los mantenimientos serán coordinados con la Oficina General de Tecnologías de Información, Comunicación y Estadística (TICE).

Los mantenimientos preventivos comprenden como mínimo lo siguiente:

a) Verificar los logs y bugs del equipamiento para poder corregir cualquier inconveniente encontrado.

b) Actualizar el firmware de los equipos, de ser necesario, dentro de la ventana de mantenimiento.

c) Diagnóstico y reconocimiento del buen funcionamiento (test) del equipamiento y sus componentes.

d) Limpieza integral, aplicación de limpia contactos en la parte externa de todos los componentes de hardware de los equipos según corresponda (ventiladores, fuentes, etc).

e) Ordenamiento del cableado de los equipos instalados en caso corresponda.

f) En su informe de mantenimiento debe incluir: Propuesta de mejora de la configuración y hardening en base a las mejores prácticas del fabricante. Se precisa que el contratista debe presentar el documento vigente de mejoras prácticas que tenga el fabricante, contrastando su propuesta con dicho documento.

5.2.1.2. Los trabajos de soporte técnico deben brindarse por el contratista en la modalidad de 7x24x365 por el periodo de la garantía solicitado, por lo que debe brindar un número y correo electrónico de su central de soporte para el reporte de incidencias (fallo o mal funcionamiento del equipamiento o alguna de sus funcionalidades), la misma que deberá ser registrada con la emisión de un ticket para seguimiento correspondiente. La generación del ticket debe indicar como su hora de inicio, la hora en la cual finaliza la llamada realizada por personal de la Superintendencia Nacional de Migraciones o la hora en la cual se registra la recepción del correo en el servidor de correos del contratista.

a) El soporte técnico incluye la atención de incidentes por falla de software y/o hardware y será realizado cuantas veces sea necesario durante la vigencia de la garantía, sin costo para la institución.
b) El contratista debe contar con un equipo de soporte técnico que brinde la solución técnica adecuada a los distintos incidentes suscitados en los equipos.
c) Este ticket servirá para realizar el seguimiento respectivo y escalamiento que fuere necesario.
d) Servicio de cambio de componentes con fallo por nuevos, en fiel cumplimiento de las especificaciones técnicas contenidas en el presente documento. Este servicio incluye la configuración o reconfiguración del equipamiento según sea necesario para posibilitar su correcto funcionamiento.
e) El ticket será cerrado, toda vez que se repare la avería y se obtenga la correspondiente aprobación por parte de la Superintendencia Nacional de Migraciones.
f) Debe incluir la opción de generar tickets directamente con el área de soporte del fabricante.

En caso de falla de Hardware que imposibilite el uso de la solución o alguno de sus componentes, el contratista tiene 24 horas como máximo para realizar la habilitación de la solución o del componente que presente dicha falla. Se aceptará que en caso la falla obligue al trámite del RMA con el fabricante, el contratista virtualice la solución o el componente dentro de las 24 horas solicitadas y lo deje operativo, hasta que llegue el equipo o componente de reemplazo. Se precisa que el tiempo máximo que se le otorga para el reemplazo por RMA es 60 días.

En caso de falla del software o bug en algún componente de la solución que no permita opera en condiciones normales, el contratista tiene 24 horas como máximo para darle solución.

5.2.2. SEGURIDAD GESTIONADA

Como parte de la Seguridad Gestionada el contratista debe asignar un (01) **Ingeniero residente (5x8)**, el cual tendrá como principales funciones:

a) Monitoreo y la administración compartida de la solución ofertada.

b) Habilitación e Implementación de nuevas reglas y/o políticas.

c) Actualización y/o revisión de toda la documentación asociada a la solución ofertada (incluye MOP de configuración)

d) Elaboración de reportes de KPI's respecto de aspectos de seguridad.

e) Seguimiento de tickets generados, tomados como base los eventos identificados por la solución ofertada.

f) Seguimiento a los problemas referidos a la solución ofertada (soporte técnico) y escalamiento con el fabricante según corresponda.

g) Optimizar la configuración de la solución ofertada, con el fin de mejorar los procesos de identificación de amenazas.

h) Apoyo en acciones para la solución y/o mitigación de las amenazas identificadas tomando como base la información proporcionada por la solución ofertada.

i) Otros que le sean asignados en el ámbito de la seguridad de la información.

j) Entregable del estado de la solución ofertada al término de la prestación.

El Ingeniero residente deberá estar físicamente trabajando en las Oficinas de la Superintendencia Nacional de Migraciones (Será potestad de la Superintendencia Nacional de Migraciones en caso continúen las restricciones dadas por el gobierno debido al COVID el que su trabajo sea remoto o mixto), su horario será de 8 horas diarias y deberá ser flexible entre las 7 horas y las 20 horas. El contratista debe asegurar que el monitoreo de la solución ofertada sea realizado por personal de su SOC cuando el Ingeniero residente no se encuentre en su horario laboral, dicho monitoreo debe ser en modalidad 24x7 (incluidos feriados) y ante la ocurrencia de un evento y/o incidente debe darle atención o solución según lo que haya establecido el personal de la Superintendencia Nacional de Migraciones.

La Oficina General de Tecnologías de Información, Comunicaciones y Estadística; podrá solicitar al contratista que el Ingeniero residente sea retirado y reemplazado, siendo las causales entre otras, faltas graves de ética, falta reiterativa a los reglamentos internos o por desconocimiento o falta de responsabilidad al realizar las funciones y/o actividades para las que ha sido designado. Luego de notificado el contratista, este deberá de ser retirado y remplazado en un plazo máximo de 72 horas.

Para desempeñar su trabajo la Superintendencia Nacional de Migraciones solo le brindarán el acceso a Internet, en caso requiera algo adicional debe ser proporcionado por el contratista.

El contratista debe proporcionar una (01) computadora (Desktop o AIO) con monitor de 23", así como un (1) escritorio de melanina con cajonera móvil de tres cajones, los cuales serán utilizados por el Ingeniero residente. Las dimensiones exactas y el color le serán entregados al día siguiente de la firma del contrato.

Se precisa que el contratista tiene como obligación realizar cualquier configuración adicional de mejora o cambio en las reglas o políticas que le sea solicitada, lo cual incluye la generación de scripts o conectores o similares en caso sea necesario para cumplir con lo requerido, asimismo los cambios y/o afinamiento y/o mejora y/o optimización de las configuraciones incluyen cualquier modulo o funcionalidad o característica que esta licenciada, aun cuando esta no haya sido descrita en el presente documento y sea soportada por los equipos instalados.

El tiempo máximo para que realice los cambios y/o afinamiento y/o mejora y/o optimización de las configuraciones que les sea solicitado, no debe exceder las 72 horas contabilizados desde la hora de inicio del ticket asignado por el contratista a la superintendencia Nacional de Migraciones.

5.2.3. CAPACITACIÓN

El periodo para el dictado del curso de transferencia de conocimientos en la solución ofertada, inicia a partir del día siguiente de firmada el *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad* y debe considerar lo siguiente:

a) Administración y solución de problemas (troubleshooting) del equipamiento ofertado, por lo que el contratista debe brindar el (los) curso(s) que el fabricante ofrezca y que toquen estos temas, aun cuando eso implique que el curso a dictar sea más de uno. Lo anterior será validado respecto del syllabus de los cursos publicados por el fabricante. El curso debe ser dictado con la cantidad de horas que se ofrezca en la página web del fabricante.

   Debe incluir el syllabus del curso oficial (teórico y práctico con laboratorio) de la marca ofertada.

   El(los) instructor(es) debe(n) tener certificación oficial otorgada por la marca en los equipos a ofertar.

b) "Análisis Forense" con una duración de al menos 40 horas y que incluya laboratorios y casos prácticos. El capacitador debe tener una experiencia mínima de 5 años comprobables en trabajos de análisis forense para lo cual debe presentar sus constancias o cualquier documento que evidencie lo solicitado previo a brindar la capacitación.

c) ISO 27032 Lead Cybersecurity Manager, con un mínimo de 40 horas.

El contratista debe proporcionar el material didáctico necesario (en forma impresa, y digital), el mismo que debe corresponder a la capacitación realizada.

Las capacitaciones serán desarrolladas en un centro de instrucción y/o capacitación proporcionado por el contratista, el mismo que deberá contar con los recursos necesarios para el dictado del curso como son: sistema de proyección, 01 pc por alumno, así como equipos para el desarrollo de las prácticas. Se aceptará que la capacitación sea virtual por parte del centro de instrucción, siempre y cuando se tengan acceso en línea al material didáctico incluidos los laboratorios que correspondan al curso.

Al finalizar la capacitación, el contratista debe realizar la entrega de certificados para cada uno de los cinco (05) asistentes en un plazo no mayor a los diez (10) días calendarios, el mismo que debe incluir el número de horas lectivas.

El plazo máximo para la realización de la capacitación será según lo indicado en el numeral **6.2 PLAZOS: "Prestación Accesoria-Capacitación"**.

5.3. NIVELES DE SERVICIO (SLA)

El contratista debe cumplir con lo siguiente:

Atenciones	Tiempo de solución
Soporte técnico: Incidentes por falla de software y/o hardware	24 horas como máximo
Seguridad Gestionada: Configuración adicional de mejora o cambio en las reglas o políticas que le sea solicitada.	72 horas como máximo

En caso superen los tiempos máximos indicados se aplicarán las penalidades indicadas en el **Numeral 12. (Otras penalidades)**.

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

6. PLAZO DE LAS PRESTACIÓNES

	ACTIVIDAD	PLAZO DEL CONTRATISTA
PRESTACIÓN PRINCIPAL	El CONTRATISTA realizará la **entrega de bienes.** Carta adjuntando copias de las guías de remisión y "Acta de Recepción"	Hasta los cuarenta y cinco (45) días calendario, contados a partir del día siguiente de suscrito el contrato.
	El CONTRATISTA realizará la **instalación y configuración.** Entrega del informe final" a la Superintendencia Nacional de Migraciones, según lo indicado en el numeral 7.1.	Hasta los sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato.
PRESTACIÓN ACCESORIA	Capacitación.	Hasta los ciento ochenta (180) días calendario, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*".
	Mantenimiento Preventivo y Soporte Técnico.	El mantenimiento preventivo debe realizarlo el contratista como mínimo una (01) vez al año durante el periodo de vigencia de la garantía (03 años). El soporte técnico debe brindarse en modalidad 7x24x 365 durante el periodo de vigencia de la garantía (03 años). Ambas actividades inician a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.
	Seguridad gestionada	Se realizará durante el tiempo que dure la garantía, tres (03) años, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.

7. ENTREGABLES

El contratista debe entregar toda la documentación en formato digital a través de la opción correspondiente de Mesa de Partes en el portal de la Agencia Digital; en caso lo realice de manera física debe dirigirlo a la Oficina General de Tecnologías de Información, Comunicaciones y Estadística (TICE), con copia a la Oficina General de Administración y Finanzas adjuntando el CD o DVD (02 juegos), en la siguiente dirección: Avenida España N° 610– Breña, de Lunes a Viernes, en el horario de 08:30 a.m. a 16:00 p.m.

7.1. PRESTACIÓN PRINCIPAL

7.1.1 Respecto de la actividad relacionada a la entrega de bienes:

Carta adjuntando copias de las guías de remisión y "Acta de Recepción"

7.1.2 Respecto de la actividad relacionada a la Instalación y configuración:

Debe presentar un "Informe Final", que debe contener como mínimo lo siguiente:

a) Arquitectura lógica de la implementación de la solución ofertada.

b) Configuraciones realizadas para la puesta en producción, incluido el detalle de cada una de las políticas y perfiles activados.

c) Detalle de los Dashboard con los eventos de seguridad configurados.

d) Diagrama de Interconexión física entre equipos de migraciones y la solución ofertada.

e) Se deben incluir e instalar todas las licencias o suscripciones necesarias para el cumplimiento de las características técnicas solicitadas.

f) Documento que acredite que las licencias están a nombre de la Superintendencia Nacional de Migraciones.

Se debe adjuntar el "*Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*".

7.2. PRESTACIÓN ACCESORIA

7.2.1 CAPACITACION:

Debe entregar un "Informe de la capacitación" en el cual adjunte el material digital proporcionado y una copia de los certificados entregados.

7.2.2 MANTENIMIENTO PREVENTIVO Y SOPORTE TECNICO.

Debe entregar un "Informe anual de las actividades realizadas en el mantenimiento preventivo y soporte técnico; según lo siguiente:

Mantenimiento preventivo:

Evidencia documental o fotográfica según corresponda de lo indicado en el numeral 5.2.1.1 de "5.2.1 MANTENIMIENTO PREVENTIVO Y SOPORTE TECNICO".

Soporte Técnico:

Respecto de las actividades de soporte técnico, debe presentar un listado con los incidentes reportados en el que se indique al menos, el número de ticket, el tiempo de solución y las actividades que se realizaron para darle solución.

7.2.3 SEGURIDAD GESTIONADA

Debe entregar un "Informe mensual" con las actividades realizadas de acuerdo a lo indicado en el numeral "5.2.2 SEGURIDAD GESTIONADA"

8. OTRAS OBLIGACIONES

8.1. OTRAS OBLIGACIONES DEL CONTRATISTA[25]

- **EL CONTRATISTA** está obligado a considerar como CONFIDENCIAL toda información proporcionada por **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"** a **"EL CONTRATISTA"** u obtenida por **"EL CONTRATISTA"** de **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**, independiente del canal, forma o circunstancia mediante la cual ha obtenido dicha información, en relación con las actividades comerciales pasadas, presentes o futuras, si hubieren, incluyendo pero no limitada a listados, correspondencia, memorandos, informes, archivos, servicios, medios magnéticos, u otros. **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"** no aceptará como propia ni validará información alguna que no provenga de sus canales oficiales internos.
- **EL CONTRATISTA** no usará la información de **""LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**, para propósito diferente que no sea la preparación de un entregable contemplado en el contrato o por algún pedido expreso de **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**
- **EL CONTRATISTA** será único y entero responsable por daños o perjuicios que cualquier documento relacionado con el contrato ocasione a terceros.
- **EL CONTRATISTA** no podrá generar copia de la información a la que tenga acceso sin la autorización previa y expresa por escrito de **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**
- **EL CONTRATISTA** proporcionará información a su personal o subcontratistas únicamente cuando dicho personal tenga necesidad de conocer tal información por razones del servicio proporcionada a **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**.

[25] **Absolución de la Consulta N° 3, formulada por TELEFONICA DEL PERU S.A.A.:** En el numeral 8.1 OTRAS OBLIGACIONES DEL CONTRATISTA se agregará lo siguiente: "La obligación de confidencialidad no aplicará a la información que: 1.- Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por parte del contratista.2.- Haya sido publicada con anterioridad a la fecha de la firma de contrato.3.- Sea independientemente desarrollada por el contratista, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la Entidad. 4.- Debe ser revelada para dar cumplimiento de una orden de naturaleza judicial, en cuyo caso el contratista deberá informar a la Entidad en forma inmediata a la sola recepción de la citada orden."

- **EL CONTRATISTA** adoptará cuantas medidas sean necesarias para evitar la pérdida o difusión no autorizada de cualquier documento relacionado con el contrato.
- **EL CONTRATISTA** deberá notificar de inmediato a **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"**, cualquier caso de pérdida o difusión no autorizada de información relacionada con el contrato.
- **EL CONTRATISTA** devolverá A **"LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES"** toda información obtenida o empleada con relación al contrato después de completar el servicio.
- **EL CONTRATISTA** está obligado a observar las condiciones de confidencialidad descritas en el presente documento y en el **COMPROMISO DE CONFIDENCIALIDAD** que le proporcione la Institución, a partir del día siguiente de la suscripción del contrato correspondiente y hasta por tres (03) años luego de concluido el contrato.

La obligación de confidencialidad no aplicará a la información que:

1) Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por parte del contratista.
2) Haya sido publicada con anterioridad a la fecha de la firma de contrato.
3) Sea independientemente desarrollada por el contratista, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la Entidad.
4) Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial , en cuyo caso el contratista deberá informar a la Entidad en forma inmediata a la sola recepción de la citada orden."

9. PERFIL DEL POSTOR

El postor deberá contar con un SOC propio en el territorio nacional.

El postor deberá contar con personas claves para el desarrollo del proyecto, los cuales deberán cumplir con los siguientes requisitos mínimos:

9.1. UN (01) JEFE DE PROYECTO

- Ingeniero Titulado en las carreras de Electrónica o Telecomunicaciones o Sistemas o Informática o Computación y Sistemas.
- Deberá tener Certificación oficial en gestión de proyectos (PMP o PMR).

Deberá estar a cargo de la gestión de la implementación (entrega, instalación y configuración) de la solución ofertada y será el encargado de las coordinaciones con el personal técnico de la entidad.

9.2. UN (01) ESPECIALISTA PARA LA INSTALACIÓN Y CONFIGURACIÓN[38]

- Bachiller o Título técnico o Profesional titulado en Ingeniería de Sistemas, Ingeniería Informática, Electrónica, Telecomunicaciones, Computación y/o Sistemas.

[38] **Absolución de la Consulta N° 17, formulada por TELEFONICA DEL PERU S.A.A.: Quedará de la siguiente manera:** Computación y/o Sistemas

- Certificación en Herramienta de Gestión de Eventos e Información de Seguridad otorgado por el fabricante.

9.3. UN (01) INGENIERO RESIDENTE

- Bachiller o Título técnico o Profesional titulado en Ingeniería de Sistemas, Ingeniería Informática, Electrónica, Telecomunicaciones, Computación y Sistemas.

  Poseer al menos una de las siguientes certificaciones vigentes:

  - Certificado en el componente SIEM otorgado por el fabricante.
  - CISSP - Profesional Certificado en Seguridad de Sistemas de Información.
  - Certificación de Certified Ethical Hacker.
  - GCIA (Certified Intrusion Analyst).
  - CHFI (Computer Hacking Forensic Investigator)

El grado académico y las certificaciones solicitadas para el Ingeniero residente, se acreditarán para la firma del contrato con cualquiera de los siguientes documentos: (i) copia simple del grado académico ii) copia simple de los certificados.

10. CONFORMIDADES:

La conformidad será emitida por la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística previa revisión de los entregables definidos en el numeral 7.

10.1. PRESTACIÓN PRINCIPAL.

10.1.1. Respecto de la actividad relacionada a la entrega de bienes.

Posterior a la entrega por parte del contratista de la carta indicada en el numeral "7.1.1 de 7. ENTREGABLES"

10.1.2 Respecto de la actividad relacionada a la Instalación y configuración

Posterior a la entrega por parte del contratista del "Informe Final" indicado en el numeral "7.1.2 de 7. ENTREGABLES"

10.2. PRESTACIÓN ACCESORIA DE CAPACITACION:

Posterior a la entrega por parte del contratista del "Informe de la capacitación" indicado en el numeral 7.2.1.

10.3. PRESTACIÓN ACCESORIA DE MANTENIMIENTO Y SOPORTE TECNICO

Posterior a la entrega por parte del contratista del "Informe anual de las actividades realizadas en el mantenimiento preventivo y soporte técnico, según lo indicado en el numeral 7.2.2.

10.4. PRESTACIÓN ACCESORIA DE SEGURIDAD GESTIONADA

Posterior a la entrega por parte del contratista del "Informe mensual" con las actividades realizadas según lo indicado en el numeral 7.2.3.

MIGRACIONES PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

11. FORMA DE PAGO

11.1. FORMA DE PAGO DE LA PRESTACIÓN PRINCIPAL

El pago correspondiente a la prestación principal se realizará de la siguiente forma:

11.1.1 80% respecto de la actividad relacionada a la entrega de bienes, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.1. de 10. CONFORMIDADES".

11.1.2 20% respecto de la actividad relacionada a la Instalación y configuración, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.2. de 10. CONFORMIDADES.

11.2. FORMA DE PAGO POR LAS PRESTACIONES ACCESORIAS:

Las prestaciones accesorias se pagarán conforme el siguiente detalle:

11.2.1 Capacitación: Se realizará en UNA (01) armada, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

11.2.2 Mantenimiento Preventivo y Soporte Técnico: Se realizará en un total de tres (03) armadas, las cuales se realizarán a razón de 1 pago al año durante el periodo de tres (03) años, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística (TICE).

11.2.3 Seguridad Gestionada: Se realizará un pago mensual, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

PRESTACIÓN ACCESORIA		
Componentes	**PAGOS**	**OBSERVACION**
Capacitación	100% del monto contractual de la capacitación	Previa conformidad
Mantenimiento preventivo y Soporte Técnico	40% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del primer año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del segundo año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del tercer año
Seguridad Gestionada	Mensual	Previa conformidad

12. OTRAS PENALIDADES

Cualquier retraso por los siguientes conceptos, implicara la aplicación de penalidades de acuerdo a:

N	CONCEPTO	Monto por hora o fracción adicional a lo señalado en los niveles de servicio	Observación
1	Soporte técnico: Incidentes por falla de software y/o hardware	10% de la UIT Vigente	Por cada hora o fracción que supere el tiempo máximo de solución, según lo indicado en el numeral 5.3.
2	Seguridad Gestionada: Configuración adicional de mejora o cambio en las reglas o políticas que le sea solicitada.	20% de la UIT Vigente	Por cada "12 horas o fracción" que supere el tiempo máximo de solución de 72 horas, según lo indicado en el numeral 5.3.

13. RESPONSABILIDADES POR VICIOS OCULTOS

El Contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes o servicios ofertados por un plazo de tres (03) años, contados a partir de la conformidad otorgada por la Entidad".

MIGRACIONES PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

14. REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR
B.1	FACTURACIÓN
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 2'000,000 (Dos millones de soles y 00/00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computan desde la fecha de conformidad o emisión del comprobante de pago, según corresponda [27]Se consideran bienes similares a los siguientes: Adquisición de Equipos de seguridad perimetral tales como Firewall, Firewall perimetral, Next Generation Firewall, Soluciones de Firewall Next Generation, Firewall de Aplicaciones Web, Soluciones de seguridad IPS o IDS, Correlación de eventos, plataforma SIEM, Plataforma de seguridad perimetral. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[28], 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 suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

[27] **Absolución de la Consultas N° 7, formulada por TELEFONICA DEL PERU S.A.A. y N° 38 formulada por SECURESOFT CORPORATION S.A.C:** Quedará redactado de la siguiente manera: Adquisición de Equipos de seguridad perimetral tales como Firewall, Firewall perimetral, Next Generation Firewall, Soluciones de Firewall Next Generation, Firewall de Aplicaciones Web, Soluciones de seguridad IPS o IDS, Correlación de eventos, plataforma SIEM, Plataforma de seguridad perimetral.

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

> *"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(...)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

MIGRACIONES PERÚ

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Universalización de la Salud"

	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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 8**. Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

C	**CAPACIDAD TÉCNICA Y PROFESIONAL**
C.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	<u>Requisitos</u>: 1. **Un (01) Jefe de Proyecto** • Experiencia profesional mínima de DOS (02) años en la gestión o gerencia de proyectos de TI. 2. **Un (01) Especialista para la instalación y configuración** • Experiencia profesional mínima de TRES (03) años en instalación y/o configuración y/o implementación de sistemas o soluciones o Herramientas de Gestión de Eventos e Información de Seguridad. 3. **Un (01) Ingeniero residente.** • Experiencia profesional mínima de DOS (02) años en temas relacionados a Seguridad Informática o administración de equipos de seguridad. <u>Acreditación</u>: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

MODELO

MATRIZ DE CUMPLIMIENTO DE CARACTERÍSTICA TÉCNICAS MINIMAS DE LA HERRAMIENTA DE GESTION DE EVENTOS E INFORMACION DE SEGURIDAD

Las características técnicas mínimas de la Herramienta de Gestión de Eventos e Información de Seguridad son:

	CARACTERISTICAS TÉCNICAS MÍNIMAS	N° de Folio
1	La solución debe proveer debe tener administración personalizable y basada en web: Monitoreo de Seguridad, Investigación basada en metadatos de eventos de seguridad, Reportes para Cumplimiento normativo.	
2	La solución SIEM con la que se aprovisione el servicio deberá contar con las siguientes capas respecto de la arquitectura y diseño: a) Colección. b) Administración de Logs (Log Management) c) Administración de Eventos (Event Management) d) Correlación de eventos e) Alarmas f) Manejo de Incidentes y casos g) Reportes	
3	Lo solicitado para el componente SIEM son appliance de propósito especifico los cuales deben ser de la marca de la solución ofertada. No se aceptará soluciones virtualizadas en un servidor y sobre un hypervisor.	
4	El componente SIEM de la solución debe estar basado en una base de datos relacional (RDBM) o no relacional o repositorio propietario del fabricante (BIG DATA) que garantice la gestión de su información y el manejo de las bitácoras/logs.	
5	La integridad de la base de datos o repositorio debe tener protección de los datos a través de cifrado o protegido por HASH	
6	La solución SIEM debe estar basada en una base de datos de acceso general (publico) o en la cual sea posible su acceso por aplicaciones de terceros para reporteo externo y no en bases de datos propietarias cerradas que impiden el acceso a los datos forenses (logs/paquetes, etc).	
7	Debe contar con un modelo de manejo de datos dentro de la base el cual sea modificable por configuración para permitir ajustar utilización (espacio en storage) de la capa de eventos, manejo de logs y detalles específicos a almacenar de manera granular, así como poder definir qué tipo de información "tirar" y cual almacenar por un tiempo específico.	
8	Debe permitir acceder a los logs originales (raw log data), siempre que así se desee, además de contar con la información previamente interpretada por la solución de Inteligencia del SIEM (Eventos, Alarmas e Incidentes)	
9	Debe contar con una consola administrativa misma que puede tener accesos vía Web (HTTPS).	
10	Dicha consola debe poder visualizarse en dispositivos móviles en sistemas operativos como Android e IOS (Deberá estar habilitada para "touch")	
11	La solución debe contar con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada.	
12	Debe mantener cifrado en los componentes de autenticación y en las capas de transporte de datos, opcionalmente este cifrado podrá ser desactivado en algunos componentes para proveer funcionalidades de agilización de transferencias de datos.	
13	Debe estar basado en una plataforma endurecida (Hardened) de sistema operativo Windows o Linux.	
14	Se deber poder aplicar parches al sistema operativo de manera discrecional conforme recomendaciones del fabricante y/o tercero que personalizó el sistema operativo sin impactar el rendimiento y presentación de la aplicación	
15	La solución SIEM con la que se aprovisione el servicio deberá estar dentro del cuadrante de líderes de Gartner de 2020 en Security Information and Event Management. (opcional)	

16	Debe soportar 2500 eventos por segundo y tener la capacidad de incrementar dicho valor en un 30% sin necesidad de agregar, cambiar o actualizar hardware.	
17	Los agentes deberán estar certificados por el fabricante además de disponibles para plataformas: Windows Server 2008 (64 Bits), Windows Server 2008 R2 (64 Bits), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 7 (64 Bits), Windows 8, Windows 10, Linux RedHat Enterprise	
18	La solución debe contar con agentes o un módulo independiente que permita convertirse o implementar un colector de eventos de otras plataformas. Se precisa que el colector de eventos puede ser virtualizado solo en el caso que sea requerido en una zona de colección remota (La Entidad brindará un equipo físico o virtual, siempre que este no requiera recursos mayores a 2 core de CPU, 4 GB de RAM y 100 GB de disco duro).	
19	Los agentes o módulos de la solución deben contar con la posibilidad de separar "relay hosts" (Servidores de Syslog que envían múltiples cadenas de logs detrás de ellos) y manifestarlos de manera independiente para realizar correlación correcta.	
20	Los agentes o módulos de la solución deben contar con la posibilidad de convertirse en colectores de flujos (Netflow o Jflow o sFlow o IPFIX), SNMP traps.	
21	Los agentes o la solución deben tener la posibilidad de realizar Host Activity Monitoring dentro de la solución (Al menos para servidores Windows)	
22	Los agentes o la solución deben tener la posibilidad de realizar Monitoreo en Tiempo Real, o modo batch y cuando aplique permitir políticas de Monitoreo de Registro de Windows. Se precisa que lo requerido en este punto, es que la solución a través de los agentes soporte y/o cumpla esta característica, sin embargo, no forma para del presente requerimiento la provisión o instalación de dichos agentes.	
23	De manera adicional los agentes o la solución deberán contar con la posibilidad de agendar los periodos de monitoreo de carpetas y archivos de logs con fines de poder realizar colección en horarios no productivos y su reporteo a infraestructuras de manejo de logs en horarios específicos con fines de evitar congestionamientos específicos con infraestructuras de comunicaciones para locaciones remotas. Se aceptará que en los agentes o la solución se pueda configurar que eventos (en función del dispositivo que los genera y su criticidad para la Institución) deben ser enviados en línea y que eventos puedan ser agendados para enviarse en otro horario.	
24	Los agentes, además de los puntos antes mencionados, deberán permitir la colección de mensajes vía API, Sockets, FTP, SSH, SCP o en general cualquier mecanismo disponible mediante la tecnología de BEATS.	
25	La solución SIEM, debe manejar una capa de información viva (live data) para búsquedas avanzadas y detalladas hasta por 120 días.	
26	La solución SIEM, debe contar con una capa de información en reposo (cold data) siempre permitiendo utilizar datos viejos archivados fuera de la infraestructura en reportes e investigaciones forenses inclusive hasta 6 meses.	
27	La solución SIEM, debe acoplarse mediante configuración a utilizar las soluciones de STORAGE que la institución tenga o adquiera en el futuro (NAS/SAN), sin necesidad de utilizar soluciones de almacenamiento propietarias. Lo anterior no debe representar ningún costo para la Entidad.	
28	Los logs archivados deberán tener la funcionalidad de almacenarse y deberán tener la tipificación básica de evidencia legal bajo el concepto (digital chain of custody) todo ello por medio de la no alteración y la custodia de los logs originales.	
29	La solución deberá realizar funciones normalización y mediación en su capa de administración de logs (log management) no en su capa de colección para aminorar el impacto a los equipos que realizan las funciones de colección.	
30	Se deberán poder separar archivados por entidad e infraestructura con fines de poder gestionar backups de esos archivados de manera separada sin impactar los backups generales de la plataforma, lo anterior tiene el fin de que la solución muestre un arreglo de multi tenencia (Multi-Tenant) donde las bitácoras archivadas se puedan separar de manera general por cliente, edificio o grupo, dependiendo la configuración que la Entidad requiera, sin tener que trabajar con la plataforma completa.	
31	El sistema de administración de Bitácoras deberá permitir configurar la utilización de memoria y CPU para su procesamiento (opcional)	
32	Cuando la cantidad de logs recibida sobrepase la capacidad licenciada de logs, la solución NO deberá "tirar/borrar" los logs y así asegurar su procesamiento.	

33	La solución deberá permitir realizar distribución de los logs ya procesados (por el log-manager) a una solución de un tercero para soluciones de maximización de componentes. (Ejemplo: Enviar los logs a otro manejador de eventos, pero previamente procesados)	
34	El sistema de administración de logs deberá permitir la utilización de certificados digitales específicos TLS.	
35	Debe contar con un framework o método sencillo para poder integrar nuevos dispositivos no detectados conforme necesidades futuras de la institución en cuestión de normalización de bitácoras. Este framework deberá permitir la adecuación de expresiones regulares básicas (regex) o plantillas XML para adecuar las reglas de "parsing" cortado y normalización.	
36	El sistema de administración de logs deberá contar con la posibilidad de configurar de manera discrecional, que es un evento y que no, de todos los logs que se reciben, con fines de maximizar las capacidades de análisis de información importante e información intrascendente.	
37	El sistema de administración de logs deberá contar con la posibilidad de traducir de manera automatizada y en tiempo real PAISES en vez de mostrar solo direcciones IP para los eventos que sean reenviados al sistema de administración de eventos.	
38	La solución SIEM debe brindar auto-clasificación de los datos capturados en modo estructurado con fines de brindar funcionalidades de búsquedas estructuradas (structured search), pero también brindar funcionalidades de búsqueda no estructurada, esto quiere decir que el sistema de inteligencia podrá ser consultado en función de estructuras específicas de datos conocidas pero también deberá permitir consultar datos sin conocer su estructura (unstructured search), lo anterior deberá estar presente en un producto único sin necesidad de duplicar la información.	
39	El sistema de administración de eventos deberá contar con la posibilidad de brindar una consola general para la consulta de la información en tiempo real, para realizar investigaciones forenses al pasado y tener la capacidad de mostrar una visión de tendencias hacia el futuro sobre los distintos eventos que se presenten en la plataforma.	
40	Debe permitir diseñar modelos de cálculo de riesgo basado en formulas especificas dictaminadas por la Entidad a fin de tomar decisiones acordes con la tipificación especifica de la amenaza en cuestión, tomando como base la información colectadas por los eventos basados en su criticidad y editar el valor de riesgo que por defecto tiene dicho evento.	
41	Las consolas de administración en conjunto con el sistema de administración de eventos deberán permitir la visión y búsqueda de más de 60 campos de metadatos normalizados para auto filtrado automatizado en donde puedan seleccionarse condicionales específicas.	
42	La consola de administración de la solución de administración de eventos y logs deberá permitir generar Layouts o dashboards específicos por persona e infraestructura que es la que analiza los datos, esto quiere decir que la vista general de la solución debe permitir configuraciones especificas por analista y perfil de búsqueda sin necesidad de re-configurar todo cada vez que se autentica a la misma.	
43	La consola de administración debe contar con la posibilidad de mostrar información realmente en tiempo real y no en procesamiento batch, esto quiere decir que la información que está cambiando en un aplicativo, sistema operativo o firewall debe ser virtualmente posible verla inmediatamente reflejada en la consola de administración sin esperar tiempos considerables a realizar esta tarea.	
44	La consola de administración deberá permitir ordenar "sortear" la información conforme necesidades específicas en tiempo real sin necesidad de la gestión de consultas o querys complicados.	
45	La consola de administración deberá contar con la posibilidad de agrupar eventos parecidos con fines de verlos de una manera más sencilla y no repetirlos, además de contar con la posibilidad de generar gráficos específicos de tiempo inicial y tiempo final en la que ocurrieron los eventos.	

46	La consola de administración deberá contar con vistas en tiempo real como: a) Estadísticas de eventos comunes. b) Estadísticas de eventos con IP origen. c) Estadísticas de eventos con Host origen. d) Estadísticas de eventos con IP destino (equipo que han sido impactados). e) Estadísticas de eventos con Host destino (equipo que han sido impactados). f) Estadísticas de aplicaciones impactadas. g) Estadísticas de fuente de logs específicos. h) Logs por semana, día y hora. i) Logs por tiempo y dirección.	
47	La consola de administración debe contar con la posibilidad de hacer clic sobre algunos objetos y obtener información de que simboliza en una gráfica, debe contar con un nivel máximo y mínimo de abstracción (drag-in, drag-out), de igual manera los componentes del dashboard deben de poder ser "detacheables" para manejar soluciones de video wall.	
48	La consola de administración deberá contar con la posibilidad de utilizar listas de objetos, cosas, direcciones IP, países, etc, estas listas deberán poder compartirse entre usuarios y auto administrarse dentro de la solución.	
49	57) Deberá promover una integración nativa con información de inteligencia de amenazas (Threat Intelligence) de fuentes OpenSource con un formato específico incluyendo STIX/TAXII.	
50	Deberá proporcionar un acceso rápido a información contextualizada dependiendo del tipo de dato que se haya seleccionado, por ejemplo, en caso de seleccionar una dirección IP, deberá proporcionar acciones de contexto para buscar esa IP en fuentes de inteligencia de direccionamiento o en buscadores de propósito general como Google.	
51	Las funcionalidades de correlación y normalización de datos, deberá realizarse en tiempo real de manera comprobable, evidenciando el modelo completo de normalización y tratamiento de los datos, creación de reglas y normalización de tiempo, permitiendo correlacionar datos "fuera de tiempo" incluso.	
52	El sistema deberá contar con una funcionalidad de actualización (automática o manual, dependiendo sea la necesidad) de inteligencia de parte del fabricante que por lo menos actualice formatos nuevos detectados de bitácoras, eventos nuevos y riesgosos, nuevas políticas de alertamiento, modificaciones en estándares.	
53	La consola de administración deberá proveer la funcionalidad de agrupar de manera completa dispositivos, hosts, redes y activos específicos para poder asignar locaciones, dirección de conectividad (inside, outside, local, etc) así como el nivel de riesgo de cada activo el cual estará ligado a la cantidad de eventos e importancia que cada uno de ellos refiera de manera aislada.	
54	Además de separar completamente la información de estas entidades internamente para que se habilite el concepto de "multi-tenant" SIEM.	
55	El sistema de administración de eventos deberá contar con la posibilidad de correlacionar de manera básica eventos por contenido de login, IP, histórico en tiempo.	
56	Quedará redactado de la siguiente manera: El sistema de correlación de eventos avanzado deberá contar con más de 600 reglas de correlación o políticas pre-definidas de detección de patrones.	
57	El sistema de correlación de eventos avanzado deberá ser manejado de manera completa por medio de wizards gráficos (drag and drop) o a través de opciones y menús que proporcione la WebUI, sin la necesidad de conocer lenguajes de programación para la gestión de políticas nuevas.	
58	El sistema de correlación de eventos avanzado deberá nutrirse no solo de información de eventos (limited subset) sino de flujos de datos (netflow o jflow o sflow o ipfix), logs nativos, etc para proveer la máxima capacidad de abstracción posible para la detección de amenazas complejas y advanced persistent threats.	
59	El sistema de correlación de eventos avanzado deberá permitir activar y desactivar las políticas durante un tiempo específico con fines de monitorear la utilización de CPU donde se están realizando estas comprobaciones a su vez la utilización de memoria RAM que es gastado en cada función de correlación avanzada.	
60	El sistema de correlación de eventos deberá contar con la posibilidad de agrupar las políticas que se ejecutan en tiempo real y ordenarlas para evitar errores de obtención de información una vez que se cumplen X o Y factores. (opcional)	

61	El sistema deberá integrarse de manera nativa con Microsoft Active Directory, con fines de extracción de la base total de usuarios y grupos para realizar correlación multidimensional y jerárquica.	
62	El sistema deberá proporcionar herramientas para integrarse con cualquier solución de gestión de identidades para la obtención confiable de usuarios de la institución.	
63	El sistema deberá permitir como mínimo a 4 administradores y analistas, acceder a información independiente de manera centralizada y recurrente (al mismo tiempo).	
64	El sistema deberá contar con una base de datos local de autenticaciones para manejar usuarios en caso de no desear alinearlo a la infraestructura de Microsoft Active Directory de la institución.	
65	El sistema deberá permitir desactivar de manera temporal cuentas sin necesidad de borrar toda la información de autenticación a la plataforma una vez que un empleado se le deniegue el acceso a dicha plataforma.	
66	El sistema deberá permitir manejar grupos y roles por grupo para poder manipular con mayor sencillez a los usuarios.	
67	El sistema deberá contar con la posibilidad de limitar el nivel de acceso conforme la credencial autenticada y esto concordar con el perfil asignado a cada empleado sobre el tipo de información a la cual se tiene acceso (fuentes de logs, configuraciones, etc).	
68	El sistema de administración de eventos deberá permitir configurar que datos deben ser compresos y cuáles no, en detalle de la base de datos de eventos al igual cual será el valor de compresión de los índices.	
69	El sistema de administración de eventos deberá manejar índices pre-calculados para agilizar las investigaciones.	
70	La consola de administración debe brindarse por medio de web, no deberá utilizar flash o java (tecnologías que brindan un riesgo completo y que incluso el soporte por default de los principales navegadores ha sido removido por cuestión de seguridad), deberá plasmarse la tecnología que cuenta ya que se busca que esta pueda ser visualizada en tablets, celulares y computadoras sin tener que instalar plugins ni aplicaciones extras al navegador común.	
71	La consola de administración debe permitir contenidos de visualización tales como mapas de conectividad (connection maps/contextualization maps), indicadores de compromiso (IOC) y configuraciones completas por el cliente para visualizar cualquier tipo de dato que se encuentre procesado por la solución.	
72	La plataforma deberá contar con la posibilidad de construir interfaces de propósito especifico con visualizaciones especificas en tableros de ciber inteligencia con el fin de brindar visibilidad de modo general y particular de acuerdo a los requerimientos de la Entidad.	
73	El sistema de manejo de alarmas deberá proveer las funcionalidades de alertar en función de observar consideraciones, patrones y condicionales específicas en cualquiera de las capas atrás mencionadas: a) Colección. b) Administración de Logs (Log Management). c) Administración de Eventos (Event Management). d) Correlación de Eventos	
74	Las alarmas deberán de manejarse como datos aislados de incidente promoviendo las funcionalidades de dar seguimiento oportuno por medio de alertas vía correo electrónico, ejecución de programas específicos o escritura a archivos planos para procesamiento futuro con otras herramientas.	
75	El sistema de alarmas deberá integrarse de manera sencilla con Remedy, OTRS u otras herramientas, por medio de correo electrónico o archivo plano o SNMP o API o REST API, con un layout específico para que oportunamente se pueda dar seguimiento a los casos detectados.	
76	El sistema de alarmas deberá contar con un sub-sistema de remediación, para realizar actividades propias de remediación.	
77	El sistema de remediación deberá contar con un framework basado en plugins o scripts para bloquear cuentas, inyectar reglas en los firewalls, bloquear puertos en switches, apagar equipos de cómputo.	
78	El sistema de remediación deberá proporcionar Playbooks con acciones o procedimientos a seguir que puedan ser asignados según las necesidades de cada departamento de la institución.	

79	El fabricante deberá proporcionar plugins por lo menos para las siguientes actividades: a) Deshabilitar cuenta en directorio activo. b) Terminar proceso en Windows y *nix de manera remota. c) Manejo de servicios (Up, Down, Monitoring). d) Adherir objetos componentes a lista (IP, Dominio, Cosa). e) Deshabilitar cuenta local en equipo Windows. f) Inyectar políticas a Palo Alto, Checkpoint, ASA.	
80	El sistema de alarmas deberá proveer funcionalidades para notificar alarmas y que puedan segregarse en el panel del dashboard principal a placer (layouts)	
81	El sistema de alarmas y manejo de incidentes debe permitir asignar el estatus a una alarma dentro de la misma herramienta con fines de que se mantenga comunicación interna entre el personal que ocupa la herramienta para saber si una alarma ha sido escalada, se está trabajando en ella o se trataba de un falso positivo, ha sido resuelta, se continuara monitoreando o no ha sido ni será resuelta además de permitir al usuario asignar comentarios a cada momento.	
82	El sistema de alarmas y manejo de incidentes permitirá conocer cuál es el histórico (quien la toco, quien la abrió, quien la cerró, quien respondió a ella, cuando) de una alarma con fines de su futura explotación y auditoria.	
83	El sistema de alarmas contará con un compendio especifico y un set de condiciones para declarar cosas que salen de cumplimiento, por ejemplo, se debe contar con alarmas preestablecidas de rompimiento de estándares generales como PCI-DSS, ISO 27001 o ISO 27002, SOX(opcional).	
84	La solución SIEM, debe proporcionar un proceso completo desde la captura de las bitácoras, indicadores y demás datos de maquina (machine data) hasta la gestión y documentación del incidente visualizado, donde deberá proporcionar un visor de incidentes.	
85	La herramienta de manejo de casos (Case Management) deberá poder interactuar con herramientas de manejo de tickets del SOC con fines de poder realizar interacción bidireccional de las evidencias (logs, screenshots, imágenes forenses de disco, capturas de paquetes).	
86	La herramienta de manejo de casos (Case Management) deberá promover un escenario jerárquico de dictaminación de incidentes en el cual se pueda asignar riesgo, colaboradores, analistas y staff que no debe de visualizar un dato específico. Lógicamente la herramienta de manejo de casos debe interactuar con el sistema de remediación para por medio de flujos de trabajo (workflows) poder responder a un incidente.	
87	La solución SIEM deberá contar con la posibilidad de generar reportes avanzados de los siguientes estándares con la adecuación completa a requerimientos de auditoria en caso de existir: a) HIPAA. b) ISO 27001 o ISO 27002. c) PCI-DSS . d) SOX	
88	La solución SIEM deberá contar con reportes de estándares y plantillas modificables por el usuario de categorías como las siguientes: a) Tops atacantes b) Vulnerabilidades c) Amenazas d) Alarmas detonadas e) Violaciones de cumplimiento f) Fallos operativos g) Violaciones de auditoria h) Reportes ejecutivos i) Detalles de logs (volumen, detalle, capacidad) j) Estadísticas de los componentes de la solución (Log Management, Event Management) k) Resúmenes y templates específicos	
89	La solución SIEM, debe mostrar los reportes en pantalla antes de solicitar cualquier exportación a formatos externos.	

90	La solución SIEM, debe guardar un registro completo de que reportes que se producen y almacenar un cache para acceso más tarde sin necesidad de ejecutar nuevamente el reporte lo cual reduce el tiempo de entrega de los mismos. Asimismo, deben exportarse a los siguientes formatos: a) CSV b) PDF	
91	Los reportes deben de contar con un análisis discrecional de privilegios dentro de la organización para solo permitir que las personas que puedan verlo sean las únicas que tienen acceso a ellos.	
92	Los reportes deberán estar visibles en la consola Web por un mínimo de 7 días y un máximo de 30 y su acceso debe ser discrecional al rol que accede a la consola.	
93	El licenciamiento debe ser basado en cantidad de Eventos por Segundo y NO en la cantidad de dispositivos que se deban integrar.	
94	La solución debe poder integrarse con soluciones de gestión de vulnerabilidades.	
95	La solución debe tener la capacidad de aprender los patrones de comportamiento de los procesos de monitoreo, a fin de mejorar los indicadores de detección temprana de las amenazas cibernéticas.	
96	La solución debe analizar el tráfico IPv4 e IPv6.	
97	La solución debe tener documentada la lista de integraciones nativas soportadas.	

[CONSIGNAR CIUDAD Y FECHA]

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

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

3.2. REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a **S/. 2´000,000.00 (Dos millones de soles y 00/100)**, por la venta de bienes 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. [9]Se consideran bienes similares a los siguientes: Adquisición de Equipos de seguridad perimetral tales como Firewall, Firewall perimetral, Next Generation Firewall, Soluciones de Firewall Next Generation, Firewall de Aplicaciones Web, Soluciones de seguridad IPS o IDS, Correlación de eventos, plataforma SIEM, Plataforma de seguridad perimetral. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[10], 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 suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

[9] **Absolución de la Consultas N° 7, formulada por TELEFONICA DEL PERU S.A.A. y N° 38 formulada por SECURESOFT CORPORATION S.A.C:** Quedará redactado de la siguiente manera: Adquisición de Equipos de seguridad perimetral tales como Firewall, Firewall perimetral, Next Generation Firewall, Soluciones de Firewall Next Generation, Firewall de Aplicaciones Web, Soluciones de seguridad IPS o IDS, Correlación de eventos, plataforma SIEM, Plataforma de seguridad perimetral.

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

> *"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(...)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

Importante
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".

C	**CAPACIDAD TÉCNICA Y PROFESIONAL**
C.1	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

1. Un (01) Jefe de Proyecto
- Experiencia profesional mínima de DOS (02) años en la gestión o gerencia de proyectos de TI.

2. Un (01) Especialista para la Instalación y configuración
- Experiencia profesional mínima de TRES (03) años en instalación y/o configuración y/o implementación de sistemas o soluciones o Herramientas de Gestión de Eventos e Información de Seguridad.

3. Un (01) Ingeniero residente.
- Experiencia profesional mínima de DOS (02) años en temas relacionados a Seguridad Informática o administración de equipos de seguridad.

Acreditación:

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

Importante

	• *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.* • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.* • *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*

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 las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el registro en el SEACE o el documento que contiene el precio de la oferta **(Anexo N° 6)**, según corresponda.	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **100 puntos**

Importante

Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de las Especificaciones Técnicas 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 de **ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM**, que celebra de una parte **SUPERINTENDENCIA NACIONAL DE MIGRACIONES**, en adelante LA ENTIDAD, con RUC Nº **20551239692,**, con domicilio legal en Av. España N° 734 del distrito de Breña de la provincia y departamento de Lima, representada por el Licenciado **IGNACIO HUGO VALLEJOS CAMPBELL**, identificado con DNI Nº 08875160, y de otra parte [.....], con RUC Nº [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA Nº** 004-2020-MIGRACIONES para la contratación de **ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM**, 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 **ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM.**

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

Este monto comprende el costo del bien, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

En caso se produzca alguna variación en el porcentaje establecido para el IGV, previa verificación de disponibilidad presupuestal por parte de la Entidad, las partes suscribirán una adenda a fin de modificar el monto contratado en igual porcentaje a la modificación del IGV introducida.[11]

CLÁUSULA CUARTA: DEL PAGO[12]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, de acuerdo al detalle, según corresponda, 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, de la manera siguiente:

[11] Absolución de la consulta N° 05 formulada por telefónica del Peru S.A.A

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

FORMA DE PAGO DE LA PRESTACIÓN PRINCIPAL

El pago correspondiente a la prestación principal se realizará de la siguiente forma:

1. 80% respecto de la actividad relacionada a la entrega de bienes, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.1. de 10. CONFORMIDADES" de las especificaciones técnicas.
2. 20% respecto de la actividad relacionada a la Instalación y configuración, posterior a la emisión de la conformidad de acuerdo a lo indicado en el numeral "10.1.2. de 10. CONFORMIDADES", de las especificaciones técnicas.

FORMA DE PAGO DE LA PRESTACIÓN ACCESORIA

Las prestaciones accesorias se pagarán conforme el siguiente detalle:

4. **Capacitación:** Se realizará en UNA (01) armada, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

5. **Mantenimiento Preventivo y Soporte Técnico:** Se realizará en un total de tres (03) armadas, las cuales se realizarán a razón de 1 pago al año durante el periodo de tres (03) años, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística (TICE).

6. **Seguridad Gestionada:** Se realizará un pago mensual, previa conformidad de la Oficina General de Tecnologías de la Información, Comunicaciones y Estadística.

PRESTACIÓN ACCESORIA		
Componentes	**PAGOS**	**OBSERVACION**
Capacitación	100% del monto contractual de la capacitación	Previa conformidad
Mantenimiento preventivo y Soporte Técnico	40% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del primer año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del segundo año
	30% del monto contractual del Mantenimiento preventivo y Soporte Técnico	Previa conformidad del tercer año
Seguridad Gestionada	Mensual	Previa conformidad

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

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, 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 se detalla, como sigue:

	ACTIVIDAD	PLAZO DEL CONTRATISTA
PRESTACIÓN PRINCIPAL	El CONTRATISTA realizará la **entrega de bienes.** Carta adjuntando copias de las guías de remisión y "Acta de Recepción"	Hasta los cuarenta y cinco (45) días calendario, contados a partir del día siguiente de suscrito el contrato.
	El CONTRATISTA realizará la **instalación y configuración.** Entrega del Informe final" a la Superintendencia Nacional de Migraciones, según lo indicado en el numeral **7.1**.	Hasta los sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato.
PRESTACIÓN ACCESORIA	Capacitación.	Hasta los ciento ochenta (180) días calendario, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*".
	Mantenimiento Preventivo y Soporte Técnico.	El mantenimiento preventivo debe realizarlo el contratista como mínimo una (01) vez al año durante el periodo de vigencia de la garantía (03 años). El soporte técnico debe brindarse en modalidad 7x24x 365 durante el periodo de vigencia de la garantía (03 años). Ambas actividades inician a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.
	Seguridad gestionada	Se realizará durante el tiempo que dure la garantía, tres (03) años, contados a partir del día siguiente de la firma del *Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*.

CLÁUSULA SEXTA :: PRESTACIONES ACCESORIAS[13]

Las prestaciones accesorias tienen por objeto atender la capacitación, mantenimiento preventivo y soporte técnico; así como la seguridad gestionada del objeto **ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM.**

El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

El plazo de ejecución de las prestaciones accesorias se da por el plazo de la garantía (03 años a partir del día siguiente de la firma del "*Acta de Instalación y configuración del equipamiento de la Herramienta de Gestión de Eventos e Información de Seguridad*").

[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS]."

CLÁUSULA SÉTIMA: 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 OCTAVA: 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.

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.

CLÁUSULA NOVENA: 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 DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA DE ALMACÉN O LA QUE HAGA SUS VECES] y la conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] 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)

[13] De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesoria(s), pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

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

CLÁUSULA UNDÉCIMA: 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 DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de TRES (3) AÑOS contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: 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.

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.

OTRAS PENALIDADES

Cualquier retraso por los siguientes conceptos, implicara la aplicación de penalidades de acuerdo a:

N	CONCEPTO	Monto por hora o fracción adicional a lo señalado en los niveles de servicio	Observación
1	Soporte técnico: Incidentes por falla de software y/o hardware	10% de la UIT Vigente	Por cada hora o fracción que supere el tiempo máximo de solución, según lo indicado en el numeral 5.3.
2	Seguridad Gestionada: Configuración adicional de mejora o cambio en las reglas o políticas que le sea solicitada.	20% de la UIT Vigente	Por cada "12 horas o fracción" que supere el tiempo máximo de solución de 72 horas, según lo indicado en el numeral 5.3.

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 CUARTA: 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 QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: 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 OCTAVA: SOLUCIÓN DE CONTROVERSIAS[14]

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 NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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"

[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).

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

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

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra[15]

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.

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

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
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) :		
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado ...			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra[16]

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

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.

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

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

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

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

iii. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.

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

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

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
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 [CONSIGNAR EL OBJETO DE LA CONVOCATORIA], de conformidad con las Especificaciones Técnicas 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 las especificaciones técnicas, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

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

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 004-2020-AF/MIGRACIONES
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **LICITACIÓN PÚBLICA N°** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO].

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]	[%][17]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%][18]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[19]

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
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
ADQUISICIÓN DE HERRAMIENTA DE GESTIÓN DE EVENTOS INFORMACIÓN DE SEGURIDAD – SIEM	**a) Prestación Principal**	
	b) Prestación Accesoria:	
	Capacitación	
	Mantenimiento Preventivo y Soporte Técnico	
	Seguridad Gestionada	
	TOTAL S/.	**(a + b)**

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 bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante
• *El postor debe consignar el precio total de la oferta, sin perjuicio, que de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
• *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*   *"Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".*

ANEXO Nº 7

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

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

1.- Que el domicilio fiscal de la empresa[20] se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);

2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);

3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y

4.- Que la empresa no tiene producción fuera de la Amazonía.[21]

[CONSIGNAR CIUDAD Y FECHA]

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

Importante
Cuando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.

[20] En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

[21] En caso de empresas de comercialización, no consignar esta condición.

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

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

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

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

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

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

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

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

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [22]	FECHA DE LA CONFORMIDAD DE SER EL CASO[23]	EXPERIENCIA PROVENIENTE[24] DE:	MONEDA	IMPORTE[25]	TIPO DE CAMBIO VENTA[26]	MONTO FACTURADO ACUMULADO [27]
4										
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 004-2020-AF/MIGRACIONES
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

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