

## ESPECIFICACIONES TÉCNICAS

### CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA GESTIÓN DE SEGURIDAD DE TI DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.



#### I. ESPECIFICACIONES TÉCNICAS

##### 1. Denominación de la contratación

Contratación de soluciones de ciberseguridad para la gestión de seguridad de TI de la infraestructura tecnológica del Ministerio de Economía y Finanzas, en el marco de la inversión con código único 2455051.

##### 2. Finalidad Pública

La Oficina General de Tecnologías de la Información (OGTI) del MEF es el órgano de administración interna encargado de planificar, implementar y gestionar sistemas de información, infraestructura tecnológica de cómputo y comunicaciones.

Es por ello que con la finalidad de garantizar la operatividad de los servicios que ofrece a sus distintos usuarios internos y externos requiere implementar soluciones de ciberseguridad para la gestión de seguridad de TI de la infraestructura tecnológica del Ministerio de Economía y Finanzas.

##### 3. Actividades POI

Fortalecimiento de la infraestructura tecnológica y ciberseguridad del MEF.

##### 4. Antecedentes

La Oficina General de Tecnologías de la Información (OGTI) del MEF, posee soluciones de protección para la red de los servicios críticos y no críticos que tiene el MEF. La antigüedad de estas soluciones es de más de 5 años y se requiere una implementación de las nuevas tecnológicas de protección que permitan hacer frente a las nuevas amenazas cibernéticas y asegurar la operatividad y disponibilidad de la red de los servicios que ofrece el MEF a sus distintos usuarios internos y externos.

##### 5. Objetivo De La Contratación

###### 5.1. Objetivo General

Contratar soluciones para gestión de riesgo de seguridad de TI de la Infraestructura Tecnológica del MEF.

###### 5.2. Objetivo Específico

- ✓ Implementar componentes de Gestión de riesgo de seguridad TI.

##### 6. Alcance y descripción de los bienes y servicios a contratar

###### 6.1. Descripción y cantidad de los bienes y servicios.

La presente adquisición está compuesta por los siguientes bienes y servicios a contratar, los mismos que se describen en los siguientes cuadros:

Solución de Gestión de Seguridad de TI		
Prestación	Descripción	Cantidad
Principal	Software de Gestión de Riesgo de Seguridad de TI	1
	<ul style="list-style-type: none"><li>Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha</li><li>Capacitación</li></ul>	1



Accesorios	Servicio de continuidad operativa <ul style="list-style-type: none"> <li>• Soporte Técnico</li> <li>• Mantenimiento Preventivo</li> </ul>	1
------------	-------------------------------------------------------------------------------------------------------------------------------------------	---

## 6.2. Distribución de las soluciones

A continuación, se muestra la distribución de los componentes de las soluciones teniendo en cuenta su ubicación:

### Software de Gestión de Riesgo de seguridad de TI

- Deberá estar implementado en el centro de datos Principal.

## 7. Características de los bienes y condiciones

### 7.1. Generalidades

- ✓ El MEF requiere realizar un fortalecimiento de la ciberseguridad, para ello requiere implementar soluciones de gestión de riesgo de seguridad de TI de la infraestructura tecnológica.
- ✓ Deben ser ofertados con licenciamiento, garantías, mantenimiento, actualización y soporte técnico del fabricante por mil noventa y cinco (1095) días calendario.
- ✓ El contratista deberá realizar el levantamiento de información, instalación, configuración, pruebas y puesta en marcha de toda la infraestructura (Hardware y/o Software) propuesta, de tal forma que no presenten problema al momento de ser utilizada por los distintos usuarios internos o externos del MEF. Así como tampoco deberá crear inconvenientes de disponibilidad a las aplicaciones existentes.
- ✓ La solución deberá ser ofrecida en su versión más estable y/o avanzada. No se aceptarán versiones beta o similares.
- ✓ En ningún caso se podrá presentar soluciones que estén en etapa de obsolescencia o que hayan anunciado su "End-of-life", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos. Eso deberá ser respaldado con una carta del fabricante **o representante local en el país (Perú)**<sup>1</sup>.
- ✓ El contratista deberá proporcionar todos los accesorios necesarios para la correcta instalación e implementación de los bienes ofertados.
- ✓ El contratista será responsable de optimizar y configurar adecuadamente cada componente ofertado a satisfacción del MEF durante la etapa de instalación, es así que, en la etapa de implementación, deberá realizar una propuesta de las configuraciones basada en las buenas prácticas (alta disponibilidad, redundancia, seguridad, tolerancia a fallas), las cuales deberán ser evaluadas y aprobadas por el Entidad.
- ✓ Las migraciones se realizarán previa coordinación con el personal del MEF, estas actividades deben garantizar la disponibilidad de los servicios, por lo tanto, el MEF proporcionará ventanas de tiempo los fines de semana o días de semana, fuera del horario de oficina, para las migraciones.
- ✓ La modalidad de contratación es llave en mano, el contratista considerará el hardware, software, licencias, instalación, configuración y pruebas, necesario para el correcto funcionamiento de todo lo solicitado en las prestaciones principales.

### 7.2. Características del equipamiento, licencias, servicios

#### 7.2.1 Adquisición de equipamiento y licencias

El Contratista debe entregar el hardware y/o softwares requeridos en el **ANEXO A1**, los mismos que deben cumplir como mínimo con las siguientes características técnicas:

<sup>1</sup> Formato de pliego de absolución de consultas y observaciones numeral 18

Solución de Gestión de Seguridad de TI	
Descripción	Anexo
Características técnicas de la solución de gestión de riesgos de seguridad de TI y análisis de eventos e información	A1

**7.2.2 Implementación:** La etapa de implementación consta de levantamiento de información, instalación, configuración, pruebas y puesta en marcha.

El Contratista deberá implementar el equipamiento de hardware y/o softwares requeridos en el **Anexo A1**, a satisfacción de MEF, siendo el Contratista responsable de optimizar y configurar adecuadamente cada componente ofertado.

Durante la etapa de implementación el Contratista será responsable del levantamiento de información, instalación, configuración, pruebas y puesta en marcha del equipamiento propuesto (hardware y/o software).

**Generalidades:**

- ✓ El Contratista debe asegurar la compatibilidad, conectividad e interoperabilidad entre el hardware y/o software que integre la arquitectura requerida.
- ✓ El MEF será responsable de suministrar el espacio físico donde se alojarán los equipos, la conectividad entre los sitios y los puntos de energía eléctricos necesarios.
- ✓ La Entidad proporcionará una red LAN y SAN extendida entre los sitios.
- ✓ La Modalidad de Ejecución Contractual será llave en mano, por lo que es obligatorio suministrar, instalar, configurar y poner en funcionamiento la solución ofertada, los materiales, accesorios, los switch, licenciamiento y todo lo que resulte necesario, para dejar completamente habilitado la solución.

**Instalación de soluciones**

- ✓ Será de total y exclusiva responsabilidad del Contratista efectuar las tareas necesarias para la puesta en marcha de toda la solución y herramientas proporcionadas (Hardware y/o Software), todo el cableado y su etiquetado (energía, redes), los switch.
- ✓ Los requerimientos específicos del ítem paquete se detalla en el anexo A2

Solución de Gestión de Seguridad de TI	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	A2

**7.3. Características y actividades del servicio de capacitación:**

El servicio de capacitación podrá ser brindado de manera presencial o virtual, dando prioridad de manera virtual siempre y cuando la naturaleza lo permita. Deberá contar con las siguientes características:

- La capacitación debe ser oficial de la marca
- Debe estar enfocada en las funcionalidades a nivel de administración de todas las soluciones ofertadas.
- Debe ser impartida en idioma español, pudiéndose brindar el material en español o inglés.

- Debe estar dirigida para siete (07) personas pertenecientes a la OGTI. Cada una de las personas debe recibir una capacitación mínima de cuarenta (40) horas para la solución que compone el ítem paquete. Se aceptará un workshop adicional para completar la cantidad de horas solicitadas para la capacitación oficial, solo en caso de que la capacitación oficial no cubra las 40 horas, para lo cual el contratista deberá sustentar esto con una carta del fabricante donde indique la cantidad de horas máximas con las que cuenta la capacitación oficial, la carta del fabricante deberá ser presentada en el primer entregable de la prestación principal.
- La frecuencia debe ser mínimo tres (03) veces a la semana, de lunes a viernes y sábados. Previa aprobación de la Oficina General de Tecnologías de la Información.

### **7.3.1. Capacitación Presencial**

La capacitación presencial deberá tener las siguientes características:

- El contratista deberá coordinar con el personal de la OIT el lugar, el horario, y los días en los cuales se impartirá la capacitación.
- De realizarse la capacitación en instalaciones ajenas del MEF, el contratista debe garantizar que los equipos electrónicos y/o softwares empleados, estén funcionando debidamente
- El especialista deberá estar presente en las instalaciones de la capacitación 10 minutos antes del inicio de cada sesión.
- Debe entregar a los participantes los materiales a emplear en digital.
- Debe registrar la asistencia del personal. Se deberá contar con la firma del personal asistente.
- Debe absolver consultas relacionadas al uso de la solución ofertada.

### **7.3.2. Capacitación Virtual**

La capacitación virtual deberá tener las siguientes características:

- Las sesiones virtuales podrán ser en vivo o sesiones pre-grabadas: De ser en vivo, se deberán grabar las sesiones para posteriormente ser subidas al aula virtual, siempre y cuando no incumpla las políticas de confidencialidad y/o propiedad intelectual, teniendo como plazo hasta el día posterior de la sesión. De ser sesiones pre-grabadas, se deberá contar con un especialista en línea, el cual deberá absolver las consultas por cada módulo.

Todo el material subido al aula virtual deberá estar habilitado en un formato 24x7 por el tiempo que dure la capacitación. El aula virtual debe contar con una barra de progreso de las sesiones.

## **8. GARANTÍA COMERCIAL**

- ✓ Todos los componentes de Hardware deben incluir mil noventa y cinco (1095) días calendario de garantía con reemplazo de partes, mano de obra y servicio ON-SITIO, contado a partir del día siguiente de emita la Conformidad de la Prestación Principal.
- ✓ Todos los componentes de Software deben incluir mil noventa y cinco (1095) días calendario de licenciamiento, suscripción y/o derecho de actualizaciones, contado a partir de del día siguiente de emitida la Conformidad de la Prestación Principal.
- ✓ Para el caso de las licencias y/o suscripciones, las actualizaciones del Software deberán estar vigentes durante los mil noventa y cinco (1095) días calendario que dure la garantía del

- ✓ La garantía de los equipos suministrados será por un período de mil noventa y cinco (1095) días calendario, contando a partir del día siguiente de emitida la Conformidad de la Prestación Principal, donde el CONTRATISTA se comprometerá a sustituir o reparar durante el tiempo de garantía toda pieza reconocida como defectuosa, debido a fallas de material o defectos de fabricación. Así mismo garantizar el suministro de repuestos por mil noventa y cinco (1095) días calendario como mínimo.
- ✓ El CONTRATISTA garantiza que todos los componentes de la Plataforma Tecnológica propuesta son nuevos, sin uso, del modelo más reciente e incorporan todas las últimas mejoras en cuanto a diseño y materiales. Ningún componente podrá presentar adulteraciones ni correcciones.
- ✓ El CONTRATISTA garantiza que todos los componentes de la Plataforma Tecnológica propuesta estarán libres de defectos que puedan manifestarse durante su uso, ya sea que dichos defectos sean el resultado de alguna acción u omisión o provengan del diseño, los materiales o la mano de obra.

## 9. Reglamentos Técnicos

El proveedor debe cumplir en la implementación con lo indicado en el siguiente reglamento técnico:

- Reglamento Peruano del Código Nacional de Electricidad, aprobado mediante Resolución Ministerial N° 175-2008-MEM/DM, sobre propagación de incendios en cables o conductores.

## 10. Normas Técnicas

El proveedor debe cumplir en la implementación con lo indicado en las siguientes normas técnicas:

- TIA-568 Rev C.1 “Estándar de Cableado de telecomunicaciones para edificios comerciales”
- IEEE 802.3 1000Base-T, 10GBase-SR, 10GBase-LR.

## 11. PRESTACIÓN ACCESORIA: SERVICIO DE CONTINUIDAD OPERATIVA

Se detallan los requerimientos mínimos de la Prestación Accesorio para los bienes ofertados en la prestación principal

Los requerimientos específicos del Ítem paquete se detallan en el anexo A3.

Solución de Gestión de Seguridad de TI	
Descripción	Anexo
Servicio de continuidad operativa	A3

## 12. FUNCIONES DEL PERSONAL

Se detalla las funciones del personal:

Solución de Gestión de Seguridad de TI			
Cant.	Personal	Perfil	Actividades
1	Coordinador (Personal Clave)	<ul style="list-style-type: none"> <li>• Titulado en Administración o Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería electrónica o Ingeniería de las telecomunicaciones o Ingeniería de Computación y Sistemas o Ingeniería Informática y de Sistemas.</li> </ul>	<ul style="list-style-type: none"> <li>• Coordinar la implementación de la solución.</li> <li>• Coordinar con el encargado del área de la OGTI del MEF.</li> <li>• Coordinar con los implementadores de su empresa para el cumplimiento de los objetivos en el tiempo planificado.</li> <li>• Reportar a la OGTI los avances según el cronograma establecido en el plan de trabajo.</li> <li>• Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). No obstante, previa coordinación y aprobación de</li> </ul>

		<ul style="list-style-type: none"> <li>• Deberá contar como mínimo con los siguientes cursos y/o certificaciones: <ul style="list-style-type: none"> <li>✓ Certificación de PMP (Project Management Professional) y/o</li> <li>✓ Cursos de Especialización, Diplomados y Maestrías en Gerencia de Proyectos en base al PMI (Project Management Institute) o Diplomado de Especialización de Gerencia y Gestión de proyectos.</li> </ul> </li> <li>• Experiencia mínima de tres (03) años en: <ul style="list-style-type: none"> <li>✓ Servicios de implementación soluciones de ciberseguridad y/o;</li> <li>✓ Jefe de proyectos en soluciones de seguridad informática y/o;</li> <li>✓ Gestión de proyectos de seguridad informática.</li> </ul> </li> </ul>	<p>la Oficina General de Tecnología de la Información se podría realizar ciertas actividades de forma remota.</p> <ul style="list-style-type: none"> <li>• Deberá estar presente en todas las reuniones programadas durante la etapa de ejecución de la prestación principal.</li> </ul>
1	Implementador Principal (Personal Clave)	<ul style="list-style-type: none"> <li>• Bachiller en Ingeniería de Sistemas o Sistemas y Computación o Sistemas y Telecomunicaciones o Sistemas e Informática o Sistemas y Seguridad Informática o Software o Telecomunicaciones o Redes y Comunicaciones o Tecnologías de la Información y las Comunicaciones o Electrónica o informática o Telecomunicaciones y redes o Informática y de Sistema.</li> <li>• Certificado Oficial de nivel profesional o ingeniería o administración o experto o especialista o asociado o consultor como mínimo en soluciones de Ciberseguridad o soluciones de seguridad informática o documento equivalente emitido por el fabricante o representante local de la marca en el país (Perú), que acredite que el personal cuenta con los conocimientos necesarios para realizar la implementación de la solución ofertada. No se aceptará certificaciones de venta o pre venta.</li> </ul>	<ul style="list-style-type: none"> <li>• Análisis de los detalles técnicos de la tecnología que se va implementar, ya sean especificaciones de hardware, de software, de licenciamiento.</li> <li>• Instalación y configuración de la solución.</li> <li>• Pruebas de la solución implementada.</li> <li>• Elaboración de la documentación de la solución implementada.</li> <li>• Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). No obstante, previa coordinación y aprobación de la Oficina General de Tecnología de la Información se podría realizar ciertas actividades de forma remota.</li> <li>• Otros requerimientos asignados por el coordinador de Proyecto.</li> </ul>

		<ul style="list-style-type: none"> <li>Experiencia mínima de tres (03) años en servicios de implementación y/o soporte en soluciones de seguridad informática.</li> </ul>	
1 (*)	Implementador(es)	<ul style="list-style-type: none"> <li>Bachiller de ingeniería o técnico profesional en las carreras: Informática o Sistemas y Telecomunicaciones o Sistemas e Informática o Sistemas y Seguridad Informática o Software o Telecomunicaciones o Redes y Comunicaciones o Tecnologías de la Información y las Comunicaciones o Electrónica, o Redes y Comunicaciones o Computación e Informática o Redes y Seguridad Informática.</li> <li>Certificado Oficial de nivel profesional o ingeniería o administración o experto o especialista o asociado o consultor como mínimo en soluciones de Ciberseguridad o soluciones de seguridad informática o documento equivalente emitido por el fabricante o representante local de la marca en el país (Perú), que acredite que el personal cuenta con los conocimientos necesarios para realizar la implementación de la solución ofertada. No se aceptará certificaciones de venta o pre venta.</li> </ul>	<ul style="list-style-type: none"> <li>Levantamiento de información de la infraestructura del MEF.</li> <li>Apoyo en la instalación y configuración de la solución ofertada.</li> <li>Apoyo en la elaboración de la documentación de la solución implementada.</li> <li>Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). No obstante, previa coordinación y aprobación de la Oficina General de Tecnología de la Información se podría realizar ciertas actividades de forma remota.</li> <li>Otros requerimientos asignados por el coordinador de Proyecto.</li> </ul>

(\*)Se deja a disposición del proveedor la cantidad del personal con el cargo de (Implementador(es)) siempre y cuando cumpla con el perfil solicitado.

Acreditación:

- La experiencia del personal se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- Copia simple del Título Profesional y/o Bachiller y/o Título técnico respectivo a fin de acreditar la formación académica requerida, la cual será verificada de corresponder en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> // o en el Registro Nacional de Certificados, Grados

y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda.

- Los cursos y/o certificaciones se acreditarán con copia simple de constancias, certificados, u otros documentos que acredite fehacientemente lo solicitado, según corresponda.

**Procedimiento para cambio del personal ofrecido, por razones de caso fortuito o fuerza mayor debidamente comprobadas.**

- ✓ Para la prestación de la contratación correspondiente, el CONTRATISTA utilizará el personal calificado especificado en su oferta, no estando permitido cambios, salvo por razones de caso fortuito o fuerza mayor debidamente comprobadas, sustentando los motivos mediante un informe que refrende dicho cambio. En estos casos, el Contratista deberá proponer a la Entidad, por escrito, a través de mesa de partes para su aprobación.
- ✓ El reemplazante deberá reunir calificaciones profesionales iguales o superiores al personal requerido en las Bases.

EL CONTRATISTA será responsable de todas las indemnizaciones por reclamos de terceros y/o del personal y/o los familiares del personal que sufran daños a consecuencia de algún siniestro; así como por el incumplimiento en materia de Seguros exigidos por la Ley.

**13. CONTRATACIÓN POR ÍTEM O PAQUETE.**

La contratación se realizará mediante ítem paquete, según detalle:

Solución de Gestión de Seguridad de TI		
Prestación	Descripción	Cantidad
Principal	Software de Gestión de Riesgo de seguridad de TI	1
	<ul style="list-style-type: none"><li>• Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha</li><li>• Capacitación</li></ul>	1
Accesorio	Servicio de continuidad operativa <ul style="list-style-type: none"><li>• Soporte Técnico</li><li>• Mantenimiento Preventivo</li></ul>	1

Por motivo que los bienes y servicios se encuentran relacionados entre sí, se considera conveniente realizar una contratación por paquete, la cual conllevará a una contratación más eficiente, toda vez que se podrá obtener mejores precios por una prestación en conjunto en comparación a una prestación desgredada de un tipo de bien o servicio en particular.

**14. Modalidad de ejecución**

La ejecución será llave en mano

**15. Seguros y pólizas**

Los seguros, pólizas y elementos de seguridad deben ser para el Ítem paquete.

**15.1. Pólizas**

**Póliza por deshonestidad.** - Por un monto equivalente a **US\$ 50,000.00 (Cincuenta Mil y 00/100 Dólares Americanos)**. Las sumas aseguradas de los convenios de la póliza podrán expresarse en límite agregado anual; sin embargo, estos montos deberán utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza deberá cubrir la reposición integral de la pérdida de dinero, objetos o bienes por deshonestidad del personal asignado para la prestación, tanto de bienes propiedad del Ministerio de



Economía y Finanzas, como de terceros que se encuentren en sus instalaciones.

**Póliza de Responsabilidad Civil**, por un monto equivalente a **US\$ 50,000.00 (Cincuenta Mil y 00/100 Dólares Americanos)**, que comprenda las coberturas de Responsabilidad Civil Extracontractual y Responsabilidad Civil Patronal. La suma asegurada de la póliza podrá expresarse en límite agregado anual; sin embargo, este monto deberá utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza cubre daños materiales y/o personales incluyendo fallecimientos, de acuerdo a los siguientes casos:

**De operaciones:** Cubre la responsabilidad civil derivada de incendios y/o explosiones.

**Patronal:** Cubre la responsabilidad civil de todo el personal destacado para la realización del servicio objeto de la convocatoria.

#### **15.2. Seguro Complementario de Trabajo de Riesgo**

Los trabajadores deberán estar sujetos al Seguro Complementario de Trabajo de Riesgo.

Para lo cual el contratista deberá presentar el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente del personal que trabajará en la prestación, y deberá estar vigente durante la ejecución del servicio. El SCTR deberá ser presentado para el inicio de la prestación.

### **16. Seguridad en el trabajo**

#### **16.1. Equipos de protección personal (EPP)**

El Contratista deberá de proporcionar los correspondientes equipos de protección personal (EPP) a su personal de acuerdo a la especialidad. Se entiende que el uso de dichos equipos es de carácter obligatorio mientras se encuentre laborando en las instalaciones del Ministerio de Economía y Finanzas.

#### **16.2. Seguridad y salud en el trabajo (SST)**

Se pone en conocimiento del Reglamento Interno de Seguridad y Salud en el Trabajo, aprobado por el Comité de Seguridad y Salud en el Trabajo del Ministerio de Economía y Finanzas, Oficializado por Resolución de Secretaría General N° 045-2021-EF/43, publicado en la página Institucional.

#### **16.3. Protocolos Sanitarios**

El Contratista deberá de implementar los protocolos sanitarios y demás disposiciones dictadas por los sectores y autoridades competentes, así como las que se dicten durante el periodo de prestación.

La adecuación y la implementación de las siguientes disposiciones son requeridas para la ejecución de la prestación.

- **Decreto Supremo N° 080-2020-PCM**, Decreto Supremo que aprueba la reanudación de actividades económicas en forma gradual y progresiva dentro del marco de la declaratoria de Emergencia Sanitaria Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del COVID-19.

- **Resolución Ministerial N° 1275-2021-MINSA**, aprueba la Directiva Administrativa N° 321-MINSA/DGIESP-2021, Directiva Administrativa que establece las disposiciones para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-CoV-2, que como Anexo forma parte integrante de la presente Resolución Ministerial

Asimismo, de las disposiciones antes mencionadas, el Contratista deberá de implementar e instruir a su personal quien ejecutará los trabajos en el Ministerio, siendo este un trabajo de Bajo Riesgo, lo siguiente:

- El personal del contratista no deberá estar comprendido dentro del grupo de riesgo indicado en la Resolución Ministerial N° 1275-2021-MINSA.
- Todo trabajador o personal de contratista deberá portar los EPP y su Kit de protección para prevenir el COVID-19, que son los implementos de seguridad entregados por el contratista a sus trabajadores y que, en función a la naturaleza de sus actividades, puede incluir todos o algunos de los siguientes implementos: mascarilla, guantes de látex o de nitrilo, alcohol en gel o solución desinfectante, lentes de seguridad, cubre zapatos, gorro descartable y uniforme de trabajo de manga larga y sus equipos de protección personal relacionadas a su labor.
- El Contratista pondrá a disposición de su personal alcohol en gel para la desinfección de sus manos, así como fomentar el lavado de manos frecuentemente, en caso no se cuente con servicio higiénico donde se realiza el trabajo, dispondrá para el personal, agua, jabón y papel toalla para el lavado de las manos.
- El contratista dispondrá dentro de la zona de trabajo contenedores/tachos para los desechos de las mascarillas y guantes desechables.
- El contratista en la medida de lo posible deberá asignar a su personal herramientas y equipos de trabajo para su uso personal.
- El personal del Contratista realizará limpieza, con mayor frecuencia, de las herramientas de trabajo manuales, equipos eléctricos y otros que sean de uso compartido.
- Deberán seguir las instrucciones de utilización de los EPPs que se le entreguen y no compartirlos (guantes, lentes, mascarillas, etc) con otro personal, siendo conveniente marcar, con rotulador indeleble, sus iniciales.
- Siendo esta contratación de Bajo Riesgo, la aplicación de pruebas serológicas o moleculares para COVID-19 es potestativo, salvo que el Ministerio identifique un caso sospechoso del personal propuesto, en tal sentido se solicitará el cambio del personal, luego del reporte por el área usuario de la Entidad.

## **17. Otros documentos**

### **17.1. Para la presentación de oferta**

- ✓ Los postores deberán presentar la siguiente documentación: Folletos, brochures, certificados, capturas de pantalla de páginas web oficiales de la marca, catálogos, instructivos, hojas de datos y/o manuales técnicos del equipamiento, para acreditar las características y/o requisitos funcionales específicos y relevantes de los bienes previstos en las especificaciones técnicas conforme al Anexo A4 de las mencionadas especificaciones; para tal efecto; deberá presentar también los mencionados formatos (Anexo A4) debidamente llenados, indicando la marca, modelo, número de parte del fabricante(opcional), el documento con el que se acredita la característica y la página correspondiente,

dichos documentos se deben presentar en idioma castellano o en su defecto, acompañado de traducción.

Solo se aceptará una carta del fabricante o subsidiaria local del fabricante o representante acreditado en el país, cuando se sustente alguna característica solicitada que no se encuentren en los documentos mencionados; asimismo, se precisa que la acreditación debe ser emitida al postor y no a la Entidad.

#### **17.2. Para la suscripción del contrato**

- ✓ Documentos de la Acreditación del perfil del personal según lo solicitado en el numeral 12 de las Especificaciones Técnicas.
- ✓ Presentación de Pólizas por deshonestidad y responsabilidad Civil.
- ✓ Documentación del postor ganador que acredite la condición de fabricante directo o subsidiaria local del fabricante o representante acreditado en el país o canal autorizado para la distribución de la marca y para brindar los bienes y servicios ofertados.
- ✓ Declaración Jurada, suscrita por el representante legal del postor, con el compromiso de brindar la garantía de soporte y buen funcionamiento de la totalidad de lo ofertado.
- ✓ Carta del fabricante o representante local en el país (Perú)<sup>2</sup> donde indique que las soluciones no estén en etapa de obsolescencia o que hayan anunciado su “End-of-life”, o dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos.

#### **17.3. Para el inicio de la prestación**

- ✓ Presentación de Seguro Complementario de Trabajo de Riesgo (SCTR) vigente del personal que trabajara en la prestación.
- ✓ Lista del personal que realizará la instalación, nombre completo y DNI.
- ✓ El contratista deberá de presentar la Ficha de sintomatología COVID-19 (Anexo 2) de la Resolución Ministerial N° 1275-2021-MINSA.
- ✓ El contratista debe estar en las fases de la Reanudación de Actividades, el cual deberá de presentar la aprobación o registro de su “Plan para la vigilancia, prevención y control de COVID-19 en el Trabajo” en el Sistema Integrado para COVID-19 (SICOVID-19), según Decreto Supremo N° 117-2020-PCM.

### **18. Medidas de control durante la ejecución contractual**

#### **18.1. Área que supervisara al Contratista**

Sera la Oficina de Infraestructura Tecnológica de la OGTI quien supervise al Contratista.

#### **18.2. Área que coordina con el Contratista**

Sera la Oficina de Infraestructura Tecnológica de la OGTI quien coordine con el Contratista.

#### **18.3. Área que brindará la conformidad**

La Conformidad de la prestación principal, será emitida por la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información (OGTI), en el plazo máximo de siete (7) días calendario de producida la recepción formal y completa de la documentación correspondiente.

### **19. Lugar y plazo de la prestación principal**

#### **19.1. Lugar**

---

<sup>2</sup> Formato de pliego de absolución de consultas y observaciones numeral 16

La entrega de los bienes se realizará en el almacén del Ministerio de Economía y Finanzas sito en Jr. Lampa N° 277 – Cercado de Lima

Asimismo, para el levantamiento de la información, implementación y puesta en marcha la Oficina General de Tecnología de la Información (OGTI) del MEF entregará al Contratista, mediante correo electrónico, dentro de los diez (10) primeros días calendarios a partir del día siguiente de la firma del contrato, la ubicación donde se instalarán las soluciones ofertadas, la ubicación será dentro de la ciudad de Lima Metropolitana. Sede Principal, Sede de Contingencia y Sede de Recuperación de desastres del Ministerio de Economía y Finanzas.

## **19.2. Plazo**

### **Plazo de entrega de bienes**

El plazo máximo de entrega de los bienes de la prestación principal, de las soluciones que se detallan en el Anexo A1, es de quince (15) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

### **Plazo de ejecución de la prestación principal**

El plazo máximo de ejecución de la prestación principal, para las soluciones que se detallan en el Anexo A1, noventa (90) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

## **20. Entregables**

**Para el ítem paquete deberán entregar lo siguiente:**

### **20.1. Primer Entregable:**

A partir del día siguiente de la firma del contrato el contratista contará con quince (15) días calendarios para hacer entrega del Plan de Trabajo, a través de mesa de partes del Ministerio de Economía y Finanzas (presencial o virtual) con atención de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información, en el cual deberá figurar como mínimo lo siguiente:

- Detalle (Nombres y apellidos completos, DNI, cargo) del equipo de personas que se encargará de la implementación de la solución.
- Presentación del SCTR.
- Plan de trabajo:
  - o Actividades a realizar.
  - o Plan de instalación que será ejecutado de acuerdo a las factibilidades de la Entidad, las mismas que podrían variar por causas no imputables al Contratista, en dicho plan se deberán establecer plazos mínimos y máximos para cada una de las tareas a cumplir, debiéndose discriminar las que deberá cumplir la Entidad, el Contratista en forma exclusiva, y las que deberán asumir en forma compartida.
  - o Hitos de implementación.
  - o Diagrama Gantt (Cronograma)
  - o Horarios de trabajo
  - o Configuraciones propuestas en las soluciones ofertadas.
  - o Procedimientos de inspección.
  - o Responsabilidades y consideraciones.
  - o Análisis y gestión de riesgos
    - ✓ Identificación de riesgos
    - ✓ Valoración de riesgos
    - ✓ Controles a implementar
    - ✓ Plan de vuelta atrás
- Documentación (datos de identificación) del personal responsable para las

coordinaciones administrativas para llevar el control sobre la prestación accesoria. Para dicho personal no se requiere un perfil, puesto que solo realizará coordinaciones entre la Entidad y el Contratista.

- Documentación del personal propuesto que brindará la asistencia técnica de la prestación accesoria y deberá contar como mínimo con el perfil y experiencia solicitada.
- Carta del fabricante que indique lo solicitado en el numeral 7.3 de la Prestación Principal de corresponder.

El contratista deberá realizar seguimiento permanente y aplicar las respectivas estrategias de mitigación en el proceso de implementación del servicio.

De identificarse nuevos riesgos que afecten el desarrollo de la implementación, estos deberán ser comunicados oportunamente por el contratista al personal de la Oficina General de Tecnologías de la Información (OGTI), alcanzando las acciones preventivas a realizarse.

Luego de recepcionado el Primer Entregable - Plan de Trabajo, la OGTI del MEF tendrá un plazo máximo de diez (10) días calendario para aprobarlo, de ser el caso, a través de un Acta. En caso la OGTI del MEF no esté conforme con el Plan de Trabajo, se otorgará al Contratista un plazo para subsanación no menor de dos (02) ni mayor de ocho (08) días, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. En caso el Contratista se exceda los plazos de presentación del Plan de Trabajo o subsanación del mismo, se aplicará penalidad a los días de exceso, acorde a lo indicado en el numeral 24 del presente documento.

#### **20.2. Segundo Entregable:**

A partir del día siguiente de suscrito el contrato el contratista contará con quince (15) días calendarios para hacer la entrega de todos los bienes. El contratista, deberá entregar el inventario y copia de los documentos de recepción de los bienes entregados a través de mesa de partes del Ministerio de Economía y Finanzas (presencial o virtual) con atención de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información.

Luego de recepcionado el Segundo Entregable, la OGTI del MEF tendrá un plazo máximo de diez (10) días calendario para aprobarlo, de ser el caso, a través de un Acta. En caso la OGTI del MEF no esté conforme con el Segundo Entregable, se otorgará al Contratista un plazo para subsanación no menor de dos (02) ni mayor de ocho (08) días, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. En caso el Contratista se exceda los plazos de presentación del Segundo Entregable o subsanación del mismo, se aplicará penalidad a los días de exceso, acorde a lo indicado en el presente documento.

#### **20.3. Tercer Entregable:**

Dentro del plazo de ejecución de la prestación principal, se deberá entregar un Informe Final, a través de mesa de partes del Ministerio de Economía y Finanzas (presencial o virtual) con atención de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información, necesario para que se otorgue la conformidad, donde se indique lo siguiente:

- Trabajos/actividades realizadas.
- Actas de avances de los trabajos (si las hubiese).
- Diagramas físicos y lógicos implementados.
- Respaldo de las configuraciones realizadas en toda la solución ofertada.

- Documento descriptivo de configuraciones de toda la solución ofertada (HW y SW)
- Credenciales de acceso de todos los dispositivos.
- Inventario de infraestructura suministrada e instalada de hardware, software y licencias.
- Documento de garantías de los bienes entregados.
- Instructivo explicativo para apertura de casos y acceso al soporte técnico
- Cronograma propuesto para los mantenimientos preventivos de la prestación accesoria.
- Arquitectura propuesta, detallando la distribución física por sitio y la conectividad entre las soluciones ofertadas.
- Informe de Verificación de Cumplimiento de todos los requerimientos técnicos de las presentes especificaciones técnicas
- Informe de Conclusiones y Recomendaciones.
- Documento de Capacitación.
  - Nombre del personal
  - Temario
  - Cantidad de horas de la capacitación brindada.
  - Certificados de los participantes de la capacitación.

Todos los documentos antes mencionados deben ser entregados en formato físico y/o digital a excepción de los respaldos de las configuraciones y la información sensible, los cuales serán presentados solo en formato digital cifrado. Para este fin se podrá realizar el intercambio de claves públicas de cifrado

En caso la OGTI del MEF no esté conforme con el entregable, se otorgará al Contratista un plazo para subsanación no menor de dos (02) ni mayor de ocho (08) días, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. En caso el Contratista se exceda los plazos de presentación del Informe Final o subsanación del mismo, se aplicará penalidad a los días de exceso, acorde a lo indicado en el numeral 24 del presente documento.

## **21. Forma de pago**

### **Prestación Principal**

El pago se realizará en dos pagos: El primer pago correspondiente al 40% se realizará luego de la emisión de la conformidad del Segundo Entregable de la Prestación Principal, previa validación de la Oficina de Infraestructura Tecnológica de la OGTI, siempre y cuando no se haya dado el adelanto inicial de 10%, caso contrario la primera cuota será del 30%. El segundo pago correspondiente al 60% se realizará luego de la emisión de la conformidad de la Oficina de Infraestructura Tecnológica de la OGTI del Tercer entregable de la Prestación Principal. El pago se realizará al Código de Cuenta Interbancaria (CCI) del contratista en Soles, de acuerdo a lo establecido en el artículo 171° del Reglamento de la Ley de Contrataciones del Estado.

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

Primer pago:

- Recepción del Almacén.
- Conformidad de la prestación emitida por la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información (OGTI).

- Comprobante de pago.
- Presentación del Segundo Entregable

Segundo pago:

- Conformidad de la prestación emitida por la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información (OGTI).
- Comprobante de pago.
- Presentación del Tercer Entregable

Dicha documentación se presentará a través de mesa de partes del Ministerio de Economía y Finanzas (presencial o virtual).

## 22. Adelantos

La entidad podrá otorgar un adelanto directo de hasta el 10% del monto del contrato original.

El contratista debe solicitar el adelanto dentro de los siete (07) días calendarios siguientes de la suscripción del contrato, adjuntado a su solicitud la garantía por adelantos mediante Carta Fianza, acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procederá la solicitud.

La entidad debe entregar el monto solicitado dentro de los diez (10) días siguientes a la presentación de la solicitud del contratista.

## 23. Penalidades

### Penalidad por mora:

De acuerdo a lo establecido en el artículo 162° del Reglamento de la Ley de Contrataciones del Estado, 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.

## 24. Otras penalidades

Asimismo, el Ministerio de Economía y Finanzas aplicará las siguientes penalidades, de acuerdo con lo dispuesto por el artículo 161° y 163° del reglamento de la Ley de Contrataciones del Estado. La acumulación de penalidades aplicadas, hasta por un monto equivalente al diez (10%) por ciento del monto del contrato, podrá ser causal de resolución de contrato por incumplimiento.

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Por incumplimiento de participación del personal Cuando se detecte que EL CONTRATISTA envía a un personal que no está especificado en la propuesta, para el desarrollo de la actividad de implementación (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será comunicada por el MEF, quien notificará a EL CONTRATISTA sobre la falta cometida, permitiéndole que subsane la falta en un plazo máximo de veinticuatro (24) horas. Si después de aplicada la penalidad, la falta continúa, se volverá a aplicar la	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
	penalidad hasta cuando ella sea subsanada.		
3	Por Incumplimiento de entregables Cuando EL CONTRATISTA incumplió plazos en la presentación de primer entregable.	10 % de la UIT vigente por cada día de demora.	Documento del contratista.
4	Incumplimiento de los Protocolos Sanitarios	10% UIT vigente por cada ocurrencia	Informe del área usuaria.

## 25. 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 en el artículo 173° del Reglamento de la Ley de Contrataciones del Estado.

El plazo de responsabilidad del contratista es de tres (03) años contado a partir de la conformidad otorgada por el Ministerio (artículo 40° de la Ley de Contrataciones del Estado).

## 26. Confidencialidad

El Contratista deberá mantener confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, queda expresamente prohibido revelar dicha información a terceros.

Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido la prestación. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista. Si este fuera el caso, esta información es reservada, por lo tanto, el Contratista y todo su personal deberá mantener la confidencialidad de la misma. El compromiso de confidencialidad se prolonga indefinidamente aún después de terminado el proyecto y se hace extensivo al personal del Contratista aun cuando ellos hayan dejado de tener vínculo laboral con éste.

## 27. Anexos

Anexo A1	Características técnicas de la Solución de Gestión de Seguridad de TI
Anexo A2	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha
Anexo A3	Servicio de continuidad operativa
Anexo A4	Características Técnicas relevantes



## **II. Requisitos de calificación**

### **A. Experiencia del Postor en la Especialidad**

**Para el Ítem Paquete, se debe considerar lo siguiente:**

**Requisitos:**

El postor debe acreditar un monto facturado acumulado equivalente a S/ 2'000,000.00 (Dos Millones con 00/100 Soles), 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.

Se consideran similares a los siguientes:

- Venta o Adquisición de solución de Gestión de Eventos e Información.
- Venta o Adquisición de equipo correlacionador de eventos.
- Venta Adquisición de plataforma SIEM.
- Venta o Adquisición de correlacionador de eventos.
- Venta o Adquisición de equipamiento de seguridad perimetral.
- Venta o Adquisición de equipamiento de seguridad de TI.
- Venta o Adquisición seguridad perimetral.
- Venta o Adquisición de seguridad TI.
- Venta o Adquisición de solución de autenticación Multifactor.
- Venta o Adquisición de solución de Gestión de identidades.
- Venta o adquisición de protección Firewall
- Venta o adquisición con instalación de protección Firewall
- Venta o adquisición de soluciones de protección Firewall
- Venta o adquisición de IPS
- Venta o adquisición con instalación de IPS
- Venta o adquisición de soluciones de IPS
- Venta o adquisición de Firewall de Aplicaciones (WAF)
- Venta o adquisición con instalación de Firewall de Aplicaciones (WAF)
- Venta o adquisición de soluciones de Firewall de Aplicaciones (WAF)
- Venta o adquisición de Firewall de Aplicaciones (WAF)
- Venta o adquisición con instalación de Firewall de Aplicaciones (WAF)
- Venta o adquisición de soluciones de Firewall de Aplicaciones (WAF)
- Venta o adquisición de Firewall de Base de datos (DBF)
- Venta o adquisición con instalación de Firewall de Base de datos (DBF)
- Venta o adquisición de soluciones de Firewall de Base de datos (DBF)
- Venta o adquisición de Filtro de Contenido (Proxy)
- Venta o adquisición con instalación de Filtro de Contenido (Proxy)
- Venta o adquisición de soluciones de Filtro de Contenido (Proxy)
- Venta o adquisición de servidor VPN
- Venta o adquisición con instalación de servidor VPN
- Venta o adquisición de soluciones VPN
- Venta o adquisición de seguridad perimetral.
- Venta o adquisición con instalación de seguridad perimetral.
- Venta o adquisición de soluciones seguridad perimetral.
- Venta o adquisición de seguridad TI.
- Venta o adquisición con instalación de seguridad TI.
- Venta o adquisición de soluciones seguridad TI.
- Venta o adquisición de Next Generation Threat Prevention Appliance.
- Venta o adquisición con instalación de Next Generation Threat Prevention Appliance.
- Venta o adquisición de soluciones Next Generation Threat Prevention

Appliance.

- Venta o adquisición de firewall perimetral para data center
- Venta o adquisición de Next Generation Threat Prevention & Sandblast, incluye instalación y/o configuración
- Venta o adquisición de Firewall, incluye instalación y/o configuración.

**Acreditación para el Item Paquete:**

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

**B. Capacidad técnica y profesional**

**B.1. Experiencia de Personal Clave para el ítem paquete:**

Requisito

**Coordinador**

Experiencia mínima de tres (03) años en servicios de implementación y/o jefe de proyectos en soluciones de seguridad informática y/o gestión de proyectos de seguridad informática

**Implementador Principal**

Experiencia mínima de tres (03) años en servicios de implementación y/o soporte en soluciones de seguridad informática.

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.



## ANEXO A1

### SOLUCIÓN PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE TI

Firmado Digitalmente por  
VELA USCAMAYTA Henry  
Roner FAU 20131370645  
soft  
Fecha: 22/08/2023  
13:35:05 COT  
Motivo: Doy V° B°

#### I. Software de Gestión de riesgos de seguridad de TI

Se requiere para el ambiente de producción y de manera opcional 2 ambientes no productivos.

- **Componente Gestión de Cumplimiento Normativo y Corporativo**

1. Debe estar licenciada para 07 (siete) usuarios por un periodo de mil noventa y cinco (1095) días calendario. Para la interacción de encuestas, planees de recolección de datos, entre otros; deberá permitir un mínimo de 2500 usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Permitir la gestión de riesgos derivado del incumplimiento regulatorio.
5. Disponer de metodologías precargadas de incumplimiento regulatorio.
6. Permitir la gestión del conjunto de normativas que apliquen a la compañía.
7. Disponer de catálogos precargados de normativas como COBIT, ISO27001, NIST y CIS controls. Para el caso de CIS controls el cual podrá estar desarrollado y configurado por el proveedor, debiendo este contar un estándar de calidad y seguridad que deberá ser presentado en el plan de trabajo y sin ningún costo adicional.
8. Permitir gestionar hasta 36 normativas diferentes cargando sus requisitos para llevar un seguimiento.
9. Permitir el envío de encuestas a un mínimo de 2500 usuarios para la recolección de todos los datos referentes a las normativas gestionadas y sus requisitos.
10. Disponer de históricos del avance de adecuación a las normativas.
11. Disponer de gráficos e informes del estado de situación de cada normativa.
12. Disponer de evidencias que permitan relacionar los requisitos normativos con los documentos del MEF.
13. Permitir la categorización, evaluación y análisis de los Bancos de Datos del MEF
14. Permitir la gestión de riesgos de protección de datos, para la evaluación de los Bancos de Datos.
15. Disponer de metodologías precargadas de protección de datos.
16. Disponer de catálogos precargados de la Ley y Reglamento de Protección de Datos del Perú (Ley 29733)
17. Permitir el envío de encuestas a un mínimo de 2500 usuarios para la recolección de todos los datos referentes a la protección de datos. (Bancos de Datos, Riesgos, Controles, Evidencias)
18. Permitir la gestión de los derechos ARCO con workflows y alertas como mínimo a 2500 usuarios propietarios de datos.
19. Disponer de históricos del avance de adecuación a la Ley 29733.
20. Disponer de gráficos e informes del estado de situación de la Ley 29733
21. Disponer de evidencias que permitan relacionar los requisitos normativos con los documentos del MEF.
22. El modelo de implementación deberá ser "Onpremise".



Firmado  
Digitalmente por  
GADEA  
CHASNAMOTE Denis  
Arturo FAU  
20131370645 soft

- **Componente Gestión de riesgo de seguridad de TI**

1. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario y licenciado para 07 (siete) usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Debe permitir la conexión simultánea de usuarios.
5. Debe disponer de un manual de usuario del software en español.
6. Debe soportar la gestión de riesgos, gestión de seguridad de la información, gestión de la protección de datos personales según la Ley 29733 de Perú y gestión del cumplimiento corporativo; permitiendo la integración de todos estos en un solo entorno.
7. En función del tipo de usuario se podrán crear y gestionar otros usuarios, o gestionar perfiles a medida.
8. Permitir la configuración de notificaciones, a través de las cuales el usuario recibirá por correo electrónico información necesaria para el desarrollo de actividades pendientes.
9. Permitir la gestión desde una sola herramienta y que las diversas funcionalidades estén integradas entre los distintos módulos. Entre las herramientas y plataformas incluidas para la integración cabe destacar: organigrama, procesos, productos, servicios, controles, etc.
10. Permitir definir los servicios y productos implicados en el alcance. Los servicios y productos que se definan pasarán a formar parte del sistema y permitirán categorizar y tipificar todo el sistema.
11. Permitir la definición de los procesos de negocio.
12. Permitir establecer dependencias entre los diferentes procesos de negocio (Macroprocesos, procesos, subprocesos, etc.).
13. Permitir establecer dependencias entre los servicios y los procesos.
14. Permitir establecer dependencias entre los procesos y los elementos del inventario (como mínimo activos, procesos y procedimientos).
15. Permitir la definición de la estructura organizativa del cliente, es decir, los departamentos, áreas, gerencias, etc. en los que se estructura la organización.
16. Permitir utilizar los elementos definidos en la estructura organizativa para asociar servicios, procesos, empleados, etc. a una estructura concreta.
17. Permite la realización de hasta 7 análisis de riesgos diferentes (como mínimo operacional, cumplimiento, salud, trabajo, auditoría)
18. Permitir la configuración de hasta 7 metodologías diferentes para la evaluación de los riesgos.
19. Permitir la definición de diferentes dimensiones, tanto cualitativas como cuantitativas, con diferentes niveles por cada dimensión.
20. Permitir metodologías cuantitativas y cualitativas.
21. Permitir realizar la identificación de riesgos asociados a la gestión de riesgos. Cada uno de estos con sus propias características y campos. Permitiendo: a. Realizar la evaluación de riesgos a nivel inherente y a nivel residual, u otros factores. y b. Asociar controles a los riesgos analizados para obtener el riesgo residual de manera manual o automática y condicionada a ponderaciones y otros factores parametrizables.
22. Actualización automática de los riesgos al modificar la valoración de los controles asociados
23. Permitir la configuración de una metodología para la evaluación de controles.

24. Permitir la definición de niveles por cada dimensión definida en la evaluación de controles.
25. Permitir la evaluación de los riesgos considerando el resultado de la evaluación de los controles.
26. Permitir asociar controles a los riesgos analizados para obtener el riesgo residual.
27. Permitir la posibilidad de realizar diferentes Planes de Tratamiento de Riesgos para los riesgos que se vayan a tratar, así como su seguimiento.
28. Permitir realizar un seguimiento del grado de avance de implantación de los controles definidos, reportados y registrados por los usuarios responsables.
29. Permitir la configuración de dimensiones y de metodologías para la evaluación de controles.
30. Permitir registrar todos los controles y medidas que el MEF tiene implantado.
31. Permitir el análisis de la eficacia de todos los controles registrados en esta opción, en función de la metodología definida para ello.
32. Permitir asociar los controles a las amenazas/riesgos de forma que se pueda reflejar qué controles están relacionados con qué amenazas.
33. Permitir el cálculo del riesgo residual en función de los controles implantados y su eficacia.
34. Permitir la generación de históricos para comparar la evolución del análisis y gestión de riesgos a lo largo del tiempo.
35. Permitir mediante el análisis de riesgos evaluar las amenazas que afectan a cada uno de los procesos y activos.
36. Permitir la categorización de los riesgos y definir taxonomías y tipologías de ellos.
37. Dispone de catálogos de amenazas, vulnerabilidades y controles predefinidos.
38. Permite la definición de KRIs de riesgos y la relación de amenazas con incidencias y vulnerabilidades.
39. Permitir obtener resultados de riesgos en función de los Servicios, Procesos, Departamentos, Tipologías de riesgos.
40. Permitir definir y adjuntar evidencias de los controles.
41. Permitir la definición de modelos de encuestas para levantar y revisar de manera periódica la información referente a Riesgos, Controles, Planes de Acción, Evidencias.
42. Permitir el envío de encuestas como mínimo a 2500 usuarios y con la posibilidad de definir workflows de revisión y aprobación.
43. Permite realizar la proyección y simulación de los riesgos en base a diferentes criterios.
44. Permite la gestión de proveedores, y los riesgos y controles derivados de estos.
45. Permitir la configuración de campos para implementar la identificación, valoración y clasificación de los activos de información, considerando:
46. Permitir la definición de los niveles de confidencialidad, integridad y disponibilidad, entre otras dimensiones, haciendo uso de un cuestionario creado para ello, así como cualquier otra característica de los activos.
47. Permitir el cálculo del nivel de criticidad del activo de información.
48. Permitir la configuración de las categorías de elementos (servicios, procesos, personal, software, etc.) que se consideran en el inventario.
49. Permitir la configuración de dimensiones cualitativas y cuantitativas para clasificar y valorar el elemento del inventario.
50. Permitir calcular la importancia de cada activo en función de la valoración realizada en las dimensiones definidas.
51. Disponer de un módulo de dependencias que permite asociar los elementos del inventario a los diferentes productos, servicios y procesos de negocio definidos, así como asociar los elementos entre sí.

52. Permitir la definición de modelos de encuestas para levantar información sobre la identificación, clasificación y definición de criticidad de cada activo de información.
53. Permite definir y documentar los Planes de Capacidad, Planes de Disponibilidad, Planes de Continuidad.
54. Permite definir la estrategia de capacitación y formación de los empleados, seguimiento de cursos.
55. Permitir la gestión de eventos, vulnerabilidades, incidencias y problemas, a través de la utilización de estados y categorías, asociación a servicios, almacenamiento de evidencias, etc.
56. Permitir asignarlos a uno o varios empleados del MEF, de forma que la herramienta avisa mediante correo electrónico de la asignación. Permite definir Workflows de gestión automatizados.
57. Permitir realizar el seguimiento de cada evento, incidencia y problema, registrando toda la información asociada
58. Permitir consultar y proponer modificaciones del análisis de riesgos ante la ocurrencia de la eventos e incidencia.
59. Permitir reevaluar los riesgos de forma automática a partir de la ocurrencia de eventos e incidencia.
60. Permitir asociar KRIs a riesgos, de acuerdo a criterios definidos.
61. Permitir asociar KPIs a activos, de acuerdo a criterios definidos.
62. Permitir establecer diversas características para los KRIs y KPIs, tales como métricas, responsables, fórmula de cálculo, etc.
63. Permitir realizar el seguimiento de KRIs y KPIs a ser reportados por los usuarios responsables.
64. Disponer de reportes genéricos que permiten visualizar la información relevante.
65. Disponer de interfaz para diseño de reportes a requerimientos del usuario.
66. Permitir la creación de informes personalizados sobre la información de la plataforma
67. Permitir visualizar de manera gráfica los resultados obtenidos tras la realización de los análisis de riesgos a través de un listado de riesgos, mapa de calor, gráfica de burbujas, gráficas de dispersión entre otros.

- **Componente Gestión de Auditoría**

1. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario y licenciado para 07 (siete) usuarios.
2. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.
3. Debe proveer toda la infraestructura de software requerido para la implementación de la solución requerida.
4. Permitir la configuración y parametrización de metodologías de Auditoría
5. Permitir configurar la metodología de auditoría para la evaluación de los Servicios, Procesos y Activos de la organización de acuerdo a la normativa actual.
6. Permitir configurar la metodología de auditoría para la evaluación de los Riesgos de acuerdo a la normativa actual.
7. Permitir configurar la metodología de auditoría para la evaluación de los Controles de acuerdo a la normativa actual.
8. Permite automatizar la obtención de resultados de las metodologías de Auditoría de acuerdo a la normativa actual.
9. Permitir la planificación anual de auditorías
10. Permitir la planificación detallada de cada trabajo de auditoría
11. Permitir la definición de roles y equipos de trabajo de auditoría

12. Permitir la ejecución de auditorías con la información actualizada de las áreas de riesgos
13. Permitir la evaluación, análisis y adjuntado de información referente a los trabajos de auditoría
14. Permitir el adjuntado, workflows de revisión, alertas y seguimiento de Papeles de Trabajo
15. Permitir consulta y revisión de evidencias de auditoría
16. Permitir consulta y revisión de las evidencias de controles
17. Permitir descarga de información sobre la ejecución de auditorías
18. Permitir generación del informe de auditoría
19. Disponer de un panel con los tiempos de auditoría, por trabajos, por auditor, por servicios.
20. Dispone de alertas y recordatorios para los auditores.
21. Permitir la creación de 5 usuarios específicos auditores
22. Permitir el perfilado de usuarios para la definición de los roles de auditoría.



## ANEXO A2

### SERVICIO DE LEVANTAMIENTO DE INFORMACIÓN, INSTALACIÓN, CONFIGURACIÓN, PRUEBAS Y PUESTA EN MARCHA

Firmado Digitalmente por  
VELA USCAMAYTA Henry  
Roner FAU 20131370645  
soft  
Fecha: 22/08/2023  
13:35:12 COT  
Motivo: Doy V° B°

#### A. Levantamiento de Información

1. Se debe realizar el levantamiento de información de todos los componentes tecnológicos requeridos de todas las sedes de la ENTIDAD para la correcta implementación de la plataforma.

#### B. Instalación y configuración

1. La Modalidad de Ejecución Contractual será llave en mano, por lo que es obligatorio suministrar, instalar, configurar y poner en funcionamiento la solución ofertada, los materiales, accesorios, los switch, licenciamiento y todo lo que resulte necesario, para dejar completamente habilitado la solución de la prestación principal.
2. Los componentes de la solución deben ser implementados en alta disponibilidad para las sedes principal y contingencia, estos también deberán integrarse con el equipamiento en alta disponibilidad que cuenta el MEF.
3. Se debe implementar la plataforma en el centro de datos del Ministerio.
4. La modalidad de contratación es llave en mano, el CONTRATISTA suministrara todo lo necesario para el correcto funcionamiento de lo solicitado en la Prestación Principal.
5. Se debe crear como mínimo un usuario por cada rol existente en la plataforma.
6. Se debe realizar otras configuraciones que el implementador considere necesario para el correcto funcionamiento de la plataforma.
7. Se debe realizar un afinamiento según las buenas prácticas recomendadas por el fabricante de la plataforma.
8. Se debe documentar todos los procedimientos realizados en la implementación.

#### C. Pruebas y puesta en marcha

1. Las inspecciones y pruebas se realizarán una vez culminadas la implementación y configuración de la solución ofertada.
2. La inspección y pruebas tiene como objetivo ejecutar los procedimientos que permitan EVIDENCIAR que los bienes (hardware y/o software) entregados por el CONTRATISTA son adecuados para el propósito del servicio y se ajustan en su totalidad a las especificaciones funcionales y/o técnicas requeridas y a las prestaciones adicionales ofrecidas por el CONTRATISTA en su oferta.
3. El CONTRATISTA propondrá a la ENTIDAD dentro del plan de trabajo, los procedimientos de inspección que serán aprobados por este último previo a su ejecución. En caso de alguna variación en la ejecución de dichos procedimientos, se debe contar con la aceptación de la ENTIDAD.
4. El CONTRATISTA y la ENTIDAD ejecutarán en forma conjunta los procedimientos de inspección.
5. Los procedimientos de inspección incluirán como mínimo:



Firmado  
Digitalmente por  
GADEA  
CHASNAMOTE Denis  
Arturo FAU  
20131370645 soft



- ✓ Detalle de las actividades a realizar por la ENTIDAD para confirmar que cada uno de los componentes de la oferta adjudicada cumple con los criterios de aceptación.
  - ✓ Detalle de las actividades a ejecutar y quién será el encargado de realizarlas, si la ENTIDAD o el CONTRATISTA.
  - ✓ Relación y datos del personal de la ENTIDAD y del CONTRATISTA que ejecutarán estos procedimientos.
6. La omisión en la oferta de algún elemento que al momento de las pruebas y a juicio de la ENTIDAD resulte necesario para el normal funcionamiento de los componentes ofrecidos, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al CONTRATISTA a proveerlo sin costo alguno para la ENTIDAD y en un plazo que no debe exceder los cinco (5) días calendario a la notificación realizada por la ENTIDAD. La ENTIDAD proveerá el acondicionamiento necesario para el alojamiento del equipamiento, siendo responsabilidad del CONTRATISTA cumplir con los objetivos de las especificaciones técnicas.
  7. Cualquier defecto notificado por la ENTIDAD al CONTRATISTA durante la realización de cualquier prueba de aceptación será inmediatamente rectificado por éste sin costo, en un plazo que no debe exceder los cinco (5) días calendario a la notificación realizada por la ENTIDAD.
  8. Culminadas las tareas de Inspección y Pruebas el CONTRATISTA deberá entregar a la OGTI los informes, manuales y procedimientos de instalación, configuración y operación de cada uno de los bienes (hardware y software) entregados, así como el Informe de Verificación de Cumplimiento de todos los requerimientos técnicos de las presentes especificaciones técnicas.



## ANEXO A3: PRESTACIÓN ACCESORIA

### CONTRATACIÓN DEL SERVICIO DE CONTINUIDAD OPERATIVA

Firmado Digitalmente por  
VELA USCAMAYTA Henry  
Roner FAU 20131370645  
soft  
Fecha: 22/08/2023  
13:35:21 COT  
Motivo: Doy V° B°

#### 1. Consideraciones generales

- Este servicio cubrirá todo el hardware y/o software ofertado.
- La prestación de este servicio es a partir del día siguiente de emitida la conformidad de la prestación principal, y tendrá una duración de mil noventa y cinco (1095) días calendario.
- El contratista deberá incluir una solución de IOC externa a la de fabricante-Base de datos externa de indicadores compromiso, por un periodo de mil noventa y cinco (1095) días calendario.
- La asistencia técnica necesaria será brindada por personal técnico calificado y especializado en los productos ofrecidos, quien deberá estar debidamente capacitado para dicha labor.
- Incluye la mano de obra y el reemplazo por repuestos originales de aquellas partes que se encuentren defectuosas.
- Las labores técnicas a realizar sobre la solución se llevarán a cabo en el lugar donde éstos se encuentren instalados. En caso sea necesario trasladar el equipo para su revisión, los gastos del envío y retorno serán por cuenta del Contratista.
- Cuando se requiera una reparación de la solución, ésta será coordinada con el personal de la OGTI del MEF.
- El Contratista no podrá alegar inconvenientes con el fabricante para la provisión de los trabajos de asistencia técnica mencionados, debiendo garantizar en toda circunstancia la posibilidad de escalamiento de los eventos.
- Los plazos de reparación de equipos, se sujetará a lo siguiente:
  - Se entiende por Tiempo de Reparación, al transcurrido entre la comunicación al Contratista sobre el mal funcionamiento del equipo (llamada de asistencia) y la reparación y puesta en funcionamiento del mismo a satisfacción de OGTI.
  - El Tiempo de Reparación máximo será de 8 horas, contabilizados desde la notificación de la falla (El tiempo de reparación máximo indicado se refiere a los equipos ofertados, la cual en el plazo indicado deberá restablecer su servicio mediante una solución definitiva o alternativa).
  - Luego de culminada cada acción correctiva, el Contratista coordinará con el personal de la OGTI para la firma de un formulario de conformidad, donde constará la información necesaria para el cálculo del tiempo de disponibilidad ("uptime") de los equipos por el funcionario responsable de OGTI.
- Las actividades técnicas podrán ser solicitadas de manera presencial o de manera remota, dando prioridad de manera remota, siempre y cuando la naturaleza de la actividad lo permita.

#### 2. Alcance y descripción del servicio

##### 2.1. Características y actividades del servicio de soporte técnico:

La prestación de este servicio es a partir del día siguiente de emitida la conformidad de la prestación principal.

##### 2.1.1. Centro de atención

- El contratista deberá contar con un centro de atención 24x7x365, al cual se podrá reportar cualquier clase de incidentes y/o requerimientos, ya sea por medio de un sistema de Mesa de Ayuda, por correo electrónico o por vía telefónica. El sistema de Mesa de Ayuda contar con mecanismos de comunicación segura como HTTPS, FTPS o SFTP.

- Debe recepcionar y registrar los incidentes y requerimientos reportados por parte del personal del MEF, así como derivar los casos reportados al responsable del soporte técnico. El ticket de atención generado debe ser único; es decir, deberá ser el mismo al momento de derivar el caso al responsable del soporte, esto con el fin de tener una mejor trazabilidad de la atención. La OGTI podrá solicitar las atenciones del servicio de soporte técnico que requiera, sin restricción de cantidad de solicitudes y sin costos adicionales.
- Para dar como terminado satisfactoriamente el servicio, debe obtener la conformidad de la atención del ticket por parte del personal de la OGTI del MEF. De darse la conformidad, se procederá a cerrar el ticket, de no darse dicha conformidad, se notificará la no conformidad al encargado del soporte técnico con el fin de revisar el motivo de la no conformidad. El cierre del ticket se realizará en centro de atención.
- El Contratista designará una persona responsable de las coordinaciones administrativas necesarias para llevar el control sobre el servicio. En caso de que exista la necesidad de comunicarse, se debe contar con datos de contacto del responsable y su jefe inmediato. Estos datos deben incluir el número de móvil, número de teléfono, anexo y correo de trabajo. Esta información debe ser constantemente revisada, actualizada y remitida por correo electrónico.
- Luego de ser atendida la solicitud, se deberá enviar por correo electrónico el informe de la atención respectiva.
- El envío de correos, reportes, documentos o de cualquier clase de información sensible por parte del Contratista hacia el Ministerio deberá estar cifrado. Para este fin se podrá realizar el intercambio de claves públicas de cifrado.

### **2.1.2. Soporte técnico**

- El Servicio de Soporte Técnico debe brindarse en modalidad 24x7x365, incluyendo fines de semana y feriados.
- Debe realizar trabajos programados que, por su envergadura, tengan que realizarse fuera de horario de oficina. Este servicio se podrá realizar de forma remota, a solicitud de la OGTI y, dependiendo de la complejidad del trabajo, se podrá solicitar la presencia del especialista en las instalaciones del MEF.
- Debe realizar el registro o reportes de incidentes, fallas, problemas y requerimientos, según corresponda, así como también realizar el seguimiento, monitoreo de la gestión de incidentes, fallas, problemas y requerimientos hasta su solución.
- Debe resolver incidentes, problemas, cambios u otros que se reporten que puedan ocasionar o pongan en riesgo la operatividad de los servicios que son resguardados por los equipos de seguridad. En caso de falla, inoperatividad o problema el contratista se encargará de corregir el mal funcionamiento o el riesgo tecnológico en los equipos de Ciberseguridad. De ser necesario, debe gestionar con el fabricante incidentes, fallas problemas o requerimientos presentados según el nivel de complejidad.
- Debe realizar revisiones diarias a nivel de las funcionalidades del sistema operativo de los dispositivos para prevenir situaciones de mal funcionamiento o un riesgo tecnológico de las plataformas, así como también realizar el monitoreo de los registros de errores (Error

logs), reportando y recomendando las acciones correctivas necesarias antes de que se produzca una falla que impida el normal funcionamiento de la solución ofertada. La entidad proporcionará los accesos correspondientes a cada necesidad.

- Debe realizar afinamiento de configuraciones, creación de políticas, copias de seguridad generación de reportes o cualquier característica correspondiente a los equipos de la solución, previo requerimiento del MEF, sin restricción de cantidad de solicitudes y sin costos adicionales. En caso se requiera actualizaciones de Firmware de los equipos, releases y reparaciones (en general denominadas comercialmente como parches, temporales, fixes, etc.), cambios en la arquitectura o similares que impliquen el corte de servicio, se deberá elaborar un Plan de Trabajo el cual debe ser enviado por correo electrónico para ser revisado y aprobado por personal del MEF.
- Debe realizar trabajos programados que, por su envergadura, tengan que realizarse fuera de horario de oficina. Este servicio se podrá realizar de forma remota, a solicitud de la OGTI y, dependiendo de la complejidad del incidente, se podrá solicitar la presencia del especialista en las instalaciones del MEF. En caso de requerir la reparación y/o cambio de algún componente, el contratista tendrá acceso al equipo para efectos de reparación las 24 horas del día, los 7 días de la semana, previa coordinación con el personal de la OGTI del MEF. En caso existan problemas de acceso, serán de responsabilidad del MEF y no serán contabilizados en el tiempo de respuesta y solución.
- El envío de correos, reportes, documentos o de cualquier clase de información sensible por parte del Contratista hacia el Ministerio deberá estar cifrado. Para este fin se podrá realizar el intercambio de claves públicas de cifrado.
- El servicio debe incluir dos (02) migraciones de la solución ofertada. La Oficina General de Tecnología de la Información (OGTI) del MEF entregará al Contratista mediante correo electrónico, la ubicación donde se migrarán los equipos ofertados. La ubicación será dentro de la ciudad de Lima Metropolitana.

## 2.2. Características y actividades del servicio de mantenimiento preventivo:

- El mantenimiento preventivo se realizará sobre los bienes adquiridos, dos veces al año, previa presentación del Plan de Trabajo por correo electrónico, según la siguiente tabla:

Mantenimiento	1	2	3	4	5	6
Mes	6	11	18	23	30	35

- La prestación de este servicio se brindará en los meses detallados en la tabla, contados a partir del día siguiente de emitida la conformidad de la prestación principal.
- El mantenimiento preventivo de hardware es a todo costo, debe ser asumido íntegramente por el contratista y debe comprender como mínimo lo siguiente: mano de obra, materiales para la limpieza, reemplazos preventivos de repuestos, partes y piezas originales y nuevos, certificados por el fabricante de la marca del equipo afectado (se verificará que estos productos se encuentren en cajas selladas y

apropiadamente embaladas por el fabricante antes de su instalación).

- Instalaciones de actualizaciones del Sistema Operativo/Firmware, así como también la verificación de la instalación del sistema operativo asociados a la solución se efectuarán a petición del MEF. De realizar actualizaciones, estas deben incluir los componentes de Firmware.
- Debe realizar la limpieza integral de todos los bienes adquiridos, así como también revisar y evaluar el estado del Hardware y/o Software de los equipos materia del presente contrato. El contratista, de detectar un imperfecto o anomalía deberá realizar cualquier ajuste necesario para su corrección a nivel de hardware y/o software.
- Si como producto del servicio, uno o varios equipos no queden operativos o algunos accesorios, partes, piezas, y/o repuestos, incluso las consideradas como consumibles (de ser el caso) resultase el dañada, impidiendo el normal y correcto funcionamiento del equipo, se deberá de realizar el cambio correspondiente a fin de que el equipo esté operativo al inicio de las labores de la entidad, teniendo como límite de tiempo para la puesta en funcionamiento del equipo, una (01) hora antes del inicio de labores de la entidad (de lunes a sábado el inicio de labores es a las 8:00 am), aplicándose las penalidades correspondientes.
- Por consideraciones de disponibilidad de los equipos, a efectos del mantenimiento preventivo de hardware, este servicio se realizará los días sábados, domingos o feriados, previa coordinación con la OGTI.
- Se debe realizar un análisis de vulnerabilidades automático y manual sobre la plataforma ofertada. Las herramientas de análisis utilizadas deben ser especializadas y ser provistas por el CONTRATISTA. Todos los resultados del análisis de vulnerabilidades realizados deberán ser corregidos.
- Cada vez que se finalice la revisión preventiva de un equipo, se deberá adherir al mismo una etiqueta que identifique apropiadamente la revisión efectuada y la fecha correspondiente.

## **2.3. Entregables**

Los documentos solicitados en el presente numeral pueden ser entregados en Mesa de Partes (Presencial o Virtual) que el MEF haya habilitado para este fin.

### **2.3.1. Servicio de Soporte Técnico:**

El Informe Mensual deberá ser entregado en un plazo máximo de diez (10) días calendario a partir del día siguiente de culminado el periodo mensual, este deberá ser enviado por correo electrónico adjuntando el archivo digital del reporte de los requerimientos solicitados. En caso del Informe Trimestral, este deberá ser entregado en Mesa de Partes del MEF. Por último, el Informe de Mejoras deberá ser enviado junto al Informe Mensual, según detalle:

#### **Informe mensual:**

- Informe Mensual del Servicio de Soporte Técnico.
  - Reporte de los requerimientos solicitados especificando lo siguiente:
    - Número del ticket generado

- Descripción de la solicitud
- Descripción de la solución
- Fecha y hora del pedido de la solicitud
- Fecha y hora de la creación del ticket
- Fecha y hora de la primera respuesta
- Fecha y hora de la solución
- Estado de la solicitud
- Recomendaciones.
- El reporte en mención también se deberá presentar en hoja de cálculo con los datos requeridos anteriormente
- Informe de Mejoras
  - Propuestas de mejoras para la Solución.

#### **Informe trimestral:**

- Informe Trimestral del Servicio de Soporte Técnico.
  - Resumen de los servicios mensuales y presentación de los entregables mensuales.

#### **2.3.2. Servicio de Mantenimiento Preventivo:**

Los documentos solicitados deberán ser entregados en Mesa de Partes del MEF, en un plazo máximo de diez (10) días calendario luego de culminado el servicio de mantenimiento, según detalle:

- Informe de Servicio de Mantenimiento Preventivo.
  - Incidentes y/o problemas presentados durante la realización del servicio de mantenimiento preventivo, posibles causas y acciones tomadas para su solución.
  - Reporte del estado actual del equipo.
  - Recomendaciones.

### **3. Nivel de Servicio**

El contratista deberá entregar su procedimiento de atención cumpliendo con lo siguiente acuerdo de nivel de servicio:

#### **Acuerdo de Nivel de Servicio – SLA (Resolución de Incidentes)**

<b>Tipo de Solicitud</b>	<b>Nivel</b>	<b>SLA (Tiempo de atención – horas hábiles)</b>	<b>Observaciones</b>
<b>Incidencias</b> Corresponden a cualquier evento que cause una interrupción del servicio o una reducción	<b>Alto</b>	<b>Tiempo de respuesta:</b> 30 minutos  <b>Tiempo de solución:</b> 4 horas	Son aquellos incidentes presentados en producción de la solución que detienen o afectan la operación, colocando en riesgo la operación o el servicio brindado por el MEF a sus usuarios. Impiden el normal funcionamiento de la solución de seguridad.

de la calidad del mismo en la solución	<b>Medio</b>	<b>Tiempo de respuesta:</b> 1 hora  <b>Tiempo de solución:</b> 6 horas	Son aquellos incidentes presentados en producción sobre la solución que no detienen la operación, pero sí impiden que uno o más usuarios del MEF cumplan con sus actividades diarias.
	<b>Bajo</b>	<b>Tiempo de respuesta:</b> 1 hora  <b>Tiempo de solución:</b> 8 horas	Son aquellos incidentes presentados en producción sobre la solución que no impiden que uno o más usuarios cumplan con sus actividades diarias, pero sí les dificulta la operación.

**Tabla n° 01: Servicio de Soporte Técnico de Incidencias**

**Acuerdo de Nivel de Servicio – SLA (Resolución de Requerimientos)**

<b>Tipo de Solicitud</b>	<b>Nivel</b>	<b>SLA (Tiempo de atención – horas hábiles)</b>	<b>Observaciones</b>
<b>Requerimiento</b> Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	<b>Medio</b>	<b>Tiempo de Respuesta</b> 2 horas  <b>Tiempo de Solución</b> 12 horas	Son aquellos requerimientos tales como: solicitudes de información, reportes, dudas, cambios en la configuración, optimización de configuraciones.

**Tabla n° 02: Servicio de Soporte Técnico de Requerimiento**

Se entiende por “Tiempo de respuesta”, al tiempo transcurrido desde que se reporta el incidente vía correo electrónico, telefónica o mesa de ayuda, hasta que el contratista designa al especialista que se encargará de la solución y responde al llamado (especialista atendiendo el caso de manera presencial o remota).

Se entiende por “Tiempo de solución”, al tiempo transcurrido desde que se reporta el incidente vía correo electrónico, telefónica o mesa de ayuda, hasta que se solucione el incidente notificado.

En caso de algún incidente o requerimiento en el que la solución dependa únicamente del mismo fabricante y que la solución por parte de esta exceda los tiempos de solución requeridos, no se aplicará el tiempo de solución establecido, para lo cual el contratista deberá sustentar y evidenciar dicha situación en el correspondiente informe y corresponde a la OGTI la evaluación y consentimiento de la situación descrita.

En caso el incidente o requerimiento dependa de la programación de una ventana de tiempo aprobada por la entidad, el tiempo de solución establecido se contará desde el inicio de la ventana de tiempo, para lo cual el contratista deberá sustentar y evidenciar dicha situación en el correspondiente informe y corresponde a la OGTI la evaluación y consentimiento de la situación descrita.

#### 4. Personal para la realización de los servicios:

##### Personal de soporte y mantenimiento

El personal encargado de realizar las actividades de soporte técnico y mantenimiento preventivo podrá ser el personal propuesto como Implementador Principal o implementador(es) de la prestación principal.

En caso sea personal propuesto distinto al de la prestación principal, deberá estar certificado y/o avalado por la marca para realizar el soporte o mantenimiento de la solución. No se aceptarán certificación de venta o pre-venta.

Asimismo, deberá tener como mínimo, un año (01) de experiencia en instalación y/o mantenimiento y/o implementación y/o administración de equipos de seguridad informática y/o soporte y/o gestión y/o especialista en soluciones de seguridad informática. La misma que se acreditará con cualquiera de los siguientes documentos: (i) constancias o (ii) certificados o (iii) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Debiendo presentar a dicho personal en el plan de trabajo de la prestación principal, indicando los nombres, DNI, actividad a realizar, y adjuntando el sustento del perfil requerido.

##### Cambio de personal

El contratista podrá solicitar el cambio del personal solo por caso fortuito o fuerza mayor debidamente justificado, debiendo proponer un nuevo personal con características iguales o superiores al personal requerido en las bases, para la aprobación de la Oficina de Infraestructura Tecnológica del MEF.

El MEF se reserva el derecho de solicitar el cambio del personal asignado debiendo el contratista reemplazarlo en un plazo de diez (10) días calendario, dicho personal deberá contar características iguales o superiores al personal requerido en las bases.

#### 5. Condiciones de operación

El contratista deberá garantizar un eficiente sistema de gestión de su plataforma tecnológica. Así mismo deberá de estar en la capacidad de realizar detección de alarmas tempranas, acciones de control preventivo y correctivo, pruebas técnicas, entre otros indicadores que se les solicite.

#### 6. Penalidad

En caso se incurra en el incumplimiento del servicio, las penalidades se considerarán de acuerdo a lo estipulado en el numeral 162 del Reglamento de la Ley de Contrataciones del Estado.

#### 7. Otras penalidades

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Por Incumplimiento De Participación Del Personal Cuando se detecte que EL	10% UIT vigente por cada	Informe del área usuaria.



Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
	CONTRATISTA envía a un personal que no está especificado en la propuesta, para el desarrollo de la actividad del servicio (por cada vez detectado).	ocurrencia	
2	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será comunicada por el MEF, quien notificará a EL CONTRATISTA sobre la falta cometida, permitiéndole que subsane la falta en un plazo máximo de veinticuatro (24) horas. Si después de aplicada la penalidad, la falta continúa, se volverá a aplicar la penalidad hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
3	Por Incumplimiento De Entregables Cuando EL CONTRATISTA incumplió plazos en la presentación de entregables.	10 % de la UIT vigente por cada día de demora.	Documento del contratista
4	Incumplimiento de los Protocolos Sanitarios	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
6	Por el tiempo excedido en la atención de un incidente o requerimiento.	Según formula del Uptime	Por cada ticket de atención, el contratista deberá hacer firmar al usuario un formulario de conformidad para el cálculo del "Uptime", en el cual se debe indicar la hora de inicio y fin de cada atención.

Por cada atención, el contratista deberá hacer firmar al usuario un formulario de conformidad para el cálculo del "UPTIME".

El UPTIME es un coeficiente que mide el nivel del servicio brindado por el Contratista

Se calculará el UPTIME, en forma trimestral, de la siguiente forma:

$$\text{UPTIME} = \frac{(\text{THM} - \text{THE}) \times 100}{\text{THM}}$$

Donde:

THM = Cantidad de horas de atención brindadas por el contratista para la provisión del servicio

THE = Sumatoria de las cantidades de horas de exceso (respecto al tiempo de solución máximo establecido en las especificaciones técnicas) en que incurrió el contratista para subsanar la averías.

Ejemplo: En un trimestre determinado ocurre lo siguiente: se reportaron 3 problemas, 2 fueron atendidos excediendo los tiempos de respuesta establecidos, con 4 y 3 horas de retraso totales.

El UPTIME será:

$$\text{THM} = 24 \times 90 = 2,160 \text{ horas}$$

$$\text{THE} = 4+3 = 7 \text{ horas}$$

$$\text{UPTIME} = \frac{2160-7}{2160} = 99.7\%$$

La penalidad trimestral, estará en función al resultado del UPTIME según la siguiente tabla:

Rango de UPTIME	Penalidad(1)
>99,90%,<=99,99%	0,5. %
>99,80%,<=99,90%	1,00%
>99,70%,<=99,80%	1,50%
>99,60%,<=99,70%	2,00%
>99,50%,<=99,60%	2,50%
>99,40%,<=99,50%	3,00%
>99,30%,<=99,40%	3,50%
>99,20%,<=99,30%	4,00%
>99,10%,<=99,20%	4,50%
>99,00%,<=99,10%	5,00%
>98,90%,<=99,00%	5,50%
>98,80%,<=98,90%	6,00%
>98,70%,<=98,80%	6,50%
>98,60%,<=98,70%	7,00%
>98,50%,<=98,60%	7,50%
>98,40%,<=98,50%	8,00%
>98,30%,<=98,40%	8,50%
>98,20%,<=98,30%	9,00%
>98,10%,<=98,20%	9,50%
Menor o igual a 98,00%	10,00%

(1) Se acumula para efectos de resolver el contrato

Para el caso del ejemplo mencionado, el contratista tendrá una penalidad en el mes equivalente al 1,5%. Este porcentaje se descontará del pago trimestral a realizar.

El Ministerio podrá resolver el Contrato si el contratista acumula una penalidad igual o mayor al 10% del monto del contrato.

## **8. Lugar y plazo de ejecución de la prestación**

### **8.1. Soporte técnico y mantenimiento:**

#### **8.1.1. Lugar**

El servicio se realizará en las sedes de sitio principal, contingencia y recuperación de desastres del Ministerio de Economía y Finanzas.

#### **8.1.2. Plazo de ejecución**

La prestación accesoria se efectuará por un periodo de mil noventa y cinco (1095) días, contabilizados a partir del día siguiente de emitida la Conformidad de la Prestación Principal. El tiempo de cobertura deberá ser de lunes a domingo las 24 horas del día.

## **9. Medidas de control**

### **9.1. Área que supervisa**

Estará supervisada por la Oficina de Infraestructura Tecnológica de la OGTI.

### **9.2. Área que coordinara con el contratista**

La coordinación de las actividades que se desarrollarán en el marco del presente servicio, estarán a cargo de la Oficina de Infraestructura Tecnológica de la OGTI.

### **9.3. Área que brindara la conformidad**

El cumplimiento de las condiciones contractuales del servicio, en concordancia a los presentes Términos de Referencia, generará la conformidad del servicio emitida por la Oficina Infraestructura Tecnológica, en el plazo máximo de siete (7) días calendario de producida la recepción formal y completa de la documentación correspondiente.

## **10. Forma de pago**

El pago se realizará en soles al Código de Cuenta Interbancaria (CCI) del contratista, según lo establecido en el artículo 171° del Reglamento de la Ley de Contrataciones del Estado, de la siguiente manera:

- Para el Servicio de Soporte técnico, el pago se realizará de forma de doce (12) pagos trimestrales en partes iguales, luego de emitida la conformidad, previa presentación de cada informe trimestral.
- Para el servicio de Mantenimiento preventivo, el pago se realizará en seis (6) partes iguales según cronograma expuesto en el numeral 2.2. del presente documento, luego de emitida la conformidad, previa presentación del informe por la realización del servicio.

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

- Conformidad de la prestación efectuada emitida por la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información (OGTI).
- Comprobante de pago.
- Presentación del informe por parte del Contratista, conforme los entregables detallados en las Especificaciones Técnicas

Dicha documentación se presentará a través de mesa de partes del Ministerio de Economía y Finanzas (presencial o virtual).

## **11. Seguros y pólizas**

### **11.1. Cumplimiento de las normas de seguridad de las normas de seguridad y salud ocupacional**

En aspectos relacionados a la seguridad e higiene ocupacional, el Contratista deberá cumplir con los lineamientos establecidos en el “Reglamento Interno de Seguridad y Salud en el Trabajo” del MEF.

El personal propuesto por el Contratista para la ejecución del servicio deberá contar en forma permanente con la indumentaria y equipos de protección personal relacionados con las actividades a desarrollar y deberán portar en forma obligatoria un chaleco (sin ningún tipo de bolsillo) y un carné de identificación visible, con fotografía actualizada.

### **11.2. Pólizas**

#### **11.2.1. Póliza por deshonestidad. -**

Por un monto equivalente a **US\$ 10,000.00 (Diez Mil y 00/100 Dólares Americanos)**. Las sumas aseguradas de los convenios de la póliza podrán expresarse en límite agregado anual; sin embargo, estos montos deberán utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza deberá cubrir la reposición integral de la pérdida de dinero, objetos o bienes por deshonestidad del personal asignado al servicio, tanto de bienes propiedad del Ministerio de Economía y Finanzas, como de terceros que se encuentren en sus instalaciones.

#### **11.2.2. Póliza de Responsabilidad Civil,**

Por un monto equivalente a **US\$ 10,000.00 (Diez Mil y 00/100 Dólares Americanos)**, que comprenda las coberturas de Responsabilidad Civil Extracontractual y Responsabilidad Civil Patronal. La suma asegurada de la póliza podrá expresarse en límite agregado anual; sin embargo, este monto deberá utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza cubre daños materiales y/o personales incluyendo fallecimientos, de acuerdo a los siguientes casos:

**De operaciones:** Cubre la responsabilidad civil derivada de incendios y/o explosiones.

**Patronal:** Cubre la responsabilidad civil de todo el personal destacado para la realización del servicio objeto de la convocatoria.

### **11.3. Seguro Complementario de Trabajo de Riesgo**

Los trabajadores deberán estar sujetos al Seguro Complementario de Trabajo de Riesgo.

Para lo cual el contratista deberá presentar el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente del personal que trabajará en la prestación, y deberá estar vigente durante la ejecución del servicio. El SCTR deberá ser presentado para el inicio de la prestación.

#### **11.4. Seguridad en el trabajo**

##### **11.4.1. Equipo de Protección Personal (EPP)**

El Contratista deberá de proporcionar los correspondientes equipos de protección personal (EPP) a su personal de acuerdo a la especialidad. Se entiende que el uso de dichos equipos es de carácter obligatorio mientras se encuentre laborando en las instalaciones del Ministerio de Economía y Finanzas.

##### **11.4.2. Seguridad y Salud en el Trabajo (SST)**

Se pone en conocimiento del Reglamento Interno de Seguridad y Salud en el Trabajo, aprobado por el Comité de Seguridad y Salud en el Trabajo del Ministerio de Economía y Finanzas, Oficializado por Resolución de Secretaría General N° 007-2014-EF/43, publicado en la página Institucional.

##### **11.4.3. Protocolos Sanitarios**

El Contratista deberá de implementar los protocolos sanitarios y demás disposiciones dictados por los sectores y autoridades competentes, así como las que se dicten durante el periodo de prestación del servicio.

La adecuación y la implementación de las siguientes disposiciones son requeridas para la ejecución de servicio.

- **Decreto Supremo N° 080-2020-PCM**, Decreto Supremo que aprueba la reanudación de actividades económicas en forma gradual y progresiva dentro del marco de la declaratoria de Emergencia Sanitaria Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del COVID-19.
- **Resolución Ministerial N° 1275-2021-MINSA**, aprueba el Documento Técnico: "Lineamiento para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-COV-2" que como anexo forma parte integrante de la presente Resolución Ministerial.

Asimismo, de las disposiciones antes mencionadas, el Contratista deberá de implementar e instruir a su personal quien ejecutará servicios en el Ministerio, siendo este un trabajo de Bajo Riesgo, lo siguiente:

- El personal del contratista no deberá estar comprendido dentro del grupo de riesgo indicado en la Resolución Ministerial N° 1275-2021-MINSA.
- Todo trabajador o personal de contratista deberá portar los EPP y su Kit de protección para prevenir el COVID-19, que son los implementos de seguridad entregados por el contratista a sus trabajadores y que, en función a la naturaleza de sus actividades, puede incluir todos o algunos de los siguientes implementos: mascarilla, guantes de látex o de nitrilo, alcohol en gel o solución desinfectante, lentes de seguridad, cubre zapatos, gorro

descartable y uniforme de trabajo de manga larga y sus equipos de protección personal relacionadas a su labor.

- El Contratista pondrá a disposición de su personal alcohol en gel para la desinfección de sus manos, así como fomentar el lavado de manos frecuentemente, en caso no se cuente con servicio higiénico donde se realiza el trabajo, dispondrá para el personal, agua, jabón y papel toalla para el lavado de las manos.
- El contratista dispondrá dentro de la zona de trabajo contenedores/tachos para los desechos de las mascarillas y guantes desechables.
- El contratista en la medida de lo posible deberá asignar a su personal herramientas y equipos de trabajo para su uso personal.
- El personal del Contratista realizará limpieza, con mayor frecuencia, de las herramientas de trabajo manuales, equipos eléctricos y otros que sean de uso compartido.
- Deberán seguir las instrucciones de utilización de los EPPs que se le entreguen y no compartirlos (guantes, lentes, mascarillas, etc) con otro personal, siendo conveniente marcar, con rotulador indeleble, sus iniciales.
- Siendo esta contratación de Bajo Riesgo, la aplicación de pruebas serológicas o moleculares para COVID-19 es potestativo, salvo que el Ministerio identifique un caso sospechoso del personal propuesto, en tal sentido se solicitará el cambio de personal en no más de 3 horas de reportado por el área usuaria de la Entidad.

## **12. Otros documentos**

### **12.1. Para la suscripción del contrato**

- ✓ Presentación de Pólizas por deshonestidad y responsabilidad Civil.

## **13. Responsabilidad por vicios ocultos**

La recepción conforme de la prestación por parte de la OGTI 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 (03) años contado a partir de la conformidad otorgada por la OGTI.

## **14. Confidencialidad**

Como parte del servicio, el contratista pudiera tomar conocimiento de la información de la plataforma tecnológica y de los sistemas de información del MEF. Si este fuera el caso, esta información es reservada, por lo tanto, el contratista y todo su personal deberá mantener la confidencialidad de la misma. El compromiso de confidencialidad se prolonga indefinidamente aún después de terminado el proyecto y se hace extensivo al personal del contratista aun cuando ellos hayan dejado de tener vínculo laboral con éste.



Firmado Digitalmente por  
TAPIA DIAZ Vicente Raul  
FAU 20131370645 soft  
Fecha: 22/08/2023 16:51:06  
COT  
Motivo: Firma Digital

Firmado Digitalmente por  
VELA USCAMAYTA Henry  
Roner FAU 20131370645  
soft  
Fecha: 22/08/2023  
13:35:31 COT  
Motivo: Doy V° B°

Firmado  
Digitalmente por  
GADEA  
CHASNAMOTE Denis  
Arturo FAU  
20131370645 soft

**ANEXO A4**

**Solución de Gestión de Riesgo de seguridad de TI**

MARCA				
MODELO				
NUMERO DE PARTE DEL FABRICANTE				
CANTIDAD				
Característica	Fuente (Folletos, brochures, certificados, enlaces web, catálogos, instructivos, hojas de datos y/o manuales técnicos, o carta del fabricante.)	Pág.	Ítem, numeral, capítulo de la pagina	Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.
Características de la Solución de Gestión de Riesgo de seguridad de TI				
A. Características de Gestión de Riesgo de seguridad de TI				
1. Debe incluir todo el licenciamiento necesario en todos los componentes de la plataforma				
2. Componente de gestión de riesgo de seguridad de TI				
3. Componente de gestión de cumplimiento normativo y corporativo				
4. Componente de gestión de auditoria				