CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA GESTIÓN DE IDENTIDADES, PROTECCIÓN DE AMBIENTES VIRTUALES, TOMA DE EVIDENCIAS DIGITALES, EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE TI DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.

I. Denominación de la contratación

Contratación de soluciones de ciberseguridad para la gestión de identidades, protección de ambiente virtuales, toma de evidencias digitales, equipamiento para el centro de ciberseguridad y el centro de operaciones de TI de la infraestructura tecnológica del Ministerio de Economía y Finanzas, en el marco de la inversión con código único 2455051.

II. 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 identidades, protección de ambiente virtuales y toma de evidencias digitales de la infraestructura tecnológica del Ministerio de Economía y Finanzas.

Asimismo, implementar el equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI, donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el Ministerio de Economía y Finanzas.

III. Actividades POI

Fortalecimiento de la infraestructura tecnológica y ciberseguridad del MEF.

IV. 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 evolución acelerada de los ataques cibernéticos requiere una implementación de nuevos componentes tecnológicos de protección que permitan hacer frente a las nuevas amenazas cibernéticas orientadas específicamente a los servicios tecnológicos que ofrece el MEF a sus distintos usuarios internos y externos.

Asimismo, la complejidad de esos incidentes requiere implementar el Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI, donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el Ministerio de Economía y Finanzas.

V. Objetivo De La Contratación

V.1. Objetivo General

Contratar soluciones para la mejora de la gestión de identidades, protección de ambientes virtuales, toma de evidencias digitales de la Infraestructura Tecnológica del MEF e implementar el equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI, donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el Ministerio de Economía y Finanzas.

V.2. Objetivo Específico

- ✓ Integrar aplicaciones con una solución de identidades.
- ✓ Establecer protección para los ambientes virtuales.
- ✓ Establecer capacidades para la toma de evidencias digitales.
- ✓ Centralizar la detección y anticipación de amenazas cibernéticas
- ✓ Centralizar las actividades de coordinación y respuesta de las amenazas cibernéticas.

VI. Alcance y descripción de los bienes a contratar

Descripción y cantidad de los bienes

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

ITEM PAQUETE 01

CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA GESTIÓN DE IDENTIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 245505.		
Prestación	**Descripción**	**Cantidad**
Principal	Software de gestión de identidades, provisionamiento y roles	1
	Software de autenticación Multifactor	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

ITEM PAQUETE 02

CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.		
Prestación	**Descripción**	**Cantidad**
Principal	Solución para la Protección de Ambientes SDDC (Software Defined Data Center) - Next Generation Firewall para Vmware NSX de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente	1
	Solución para la Protección de Contenedores y Gestor de Contenedores - Prisma Cloud Compute de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

ITEM PAQUETE 03

CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA TOMA DE EVIDENCIAS DIGITALES DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051		
Prestación	**Descripción**	**Cantidad**
Principal	Software de extracción de datos de computadoras	1
	Equipo de extracción de datos de dispositivos	1
	Software de análisis de datos digitales extraídos	1
	Servidor de análisis de datos extraídos FRED	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

ITEM PAQUETE 04

CONTRATACIÓN DEL EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE TI DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.		
Prestación	**Descripción**	**Cantidad**
Principal	Piso Técnico.	2
	Sistema de Iluminación.	2
	Control de Acceso.	2
	Construcción en seco, sellado, pintura de paredes, pisos y puertas.	2
	Falso Cielo Raso	1
	Sistema de Aire Acondicionado.	1
	Gabinete de Comunicaciones.	5
	Unidad de Distribución Energética (PDUs).	12
	Conmutador de Trasferencia Automático	14
	Sistema de Video Wall (3x2).	1
	Sistema de Video Wall (4x2)	1
	Controlador de Video Wall.	2
	Workstation.	19
	Plataforma de Gestión.	1
	Mobiliarios.	19
	Sistema Eléctrico Estabilizado y Comercial.	2
	Cableado Estructurado.	2
	Detección de Incendios.	2
	Cámaras IP	5
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha.	2
Accesoria	Servicio de continuidad operativa y transferencia de conocimiento • Soporte Técnico • Mantenimiento Preventivo • Capacitación	2

Las Especificaciones Técnicas de cada ítem se detallan a continuación:

ITEM PAQUETE 01

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

ESPECIFICACIONES TÉCNICAS
CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA GESTIÓN DE IDENTIDADES 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 identidades 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 identidades 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 evolución acelerada de los ataques cibernéticos requiere una implementación de nuevos componentes tecnológicos de protección que permitan hacer frente a las nuevas amenazas cibernéticas orientadas específicamente a los servicios tecnológicos que ofrece el MEF a sus distintos usuarios internos y externos.

5. Objetivo De La Contratación

5.1 Objetivo General

Contratar soluciones para la mejora de la gestión de identidades de la Infraestructura Tecnológica del MEF.

5.2 Objetivo Específico

- ✓ Integrar aplicaciones con una solución de identidades.

6. Alcance y descripción de los bienes a contratar

6.1 Descripción y cantidad de los bienes

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

ITEM PAQUETE 01

Solución de Gestión de Identidades		
Prestación	**Descripción**	**Cantidad**
Principal	Software de gestión de identidades, provisionamiento y roles	1
	Software de autenticación Multifactor	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa	1

	• Soporte Técnico • Mantenimiento Preventivo • Capacitación	

6.2 Distribución de las soluciones

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

Ítem Paquete 01

Software de gestión de identidades, provisionamiento y roles

- Deberá estar implementado en los centros de datos Principal, Contingencia y Recuperación de Desastres.

Software de autenticación multifactor

- Deberá estar implementado en los centros de datos Principal, Contingencia y Recuperación de Desastres.

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 identidades 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 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.
- ✓ Todos los equipos deben ser nuevos, sin uso y de reciente fabricación. No se aceptarán equipos usados o re manufacturados.
- ✓ 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.
- ✓ 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 software requeridos en el **ANEXO A1**, el mismo que debe cumplir como mínimo con las siguientes características técnicas:

ITEM PAQUETE 01

Solución de Gestión de Identidades	
Descripción	Anexo
Características técnicas de la solución de gestión de identidades	A1

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

El Contratista deberá implementar el equipamiento de hardware y software 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 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 todos los servidores y herramientas proporcionadas (Hardware y Software), todo el cableado y su etiquetado (energía, redes), los switch.
- ✓ Los requerimientos específicos del ítem paquete 01 se detalla en el anexo A2.

ITEM PAQUETE 01

Ítem Paquete 01	
Solución de Gestión de Identidades	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	A2

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. Esta garantía debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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. Esto debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 equipamiento o hasta que se encuentren vigentes por el fabricante.
- ✓ La garantía de los equipos suministrados será por un período de mil noventa y cinco (1095) días calendario, después 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.
- ✓ Todos los componentes de la Plataforma Tecnológica propuesta no podrán presentar adulteraciones ni correcciones (por ejemplo: tarjeta madre, fuente, etc.).

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 Accesoria para los bienes ofertados en la prestación principal (Anexo A1)

Los requerimientos específicos en el Ítem paquete 01 se detallan en el anexo A3.

ITEM PAQUETE 01

Ítem Paquete 01	
Solución de Gestión de Identidades	
Descripción	Anexo
Servicio de continuidad operativa	A3

12. FUNCIONES DEL PERSONAL

Se detalla las funciones del personal:

ITEM PAQUETE 01

Ítem Paquete 01			
Solución de Gestión de Identidades			
Cant.	Personal	Perfil	Actividades
1	Coordinador (Personal Clave)	• Titulado en Administración o Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería electrónica o Ingeniería de las telecomunicaciones o Ingeniería de Computación y Sistemas. • Certificación de PMP (Project Management Professional). • Experiencia mínima de tres (03) años en servicios de implementación o soporte o proyectos en soluciones de seguridad informática.	• Coordinar la implementación de la solución. • Coordinar con el encargado del área de la OGTI del MEF. • Coordinar con los implementadores de su empresa para el cumplimiento de los objetivos en el tiempo planificado. • Reportar a la OGTI los avances según el cronograma establecido en el plan de trabajo. • 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.
1	Implementador I (Personal Clave)	• 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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en el componente/solución de Software de gestión de identidades, provisionamiento y roles	• Análisis de los detalles técnicos de la tecnología que se va implementar, ya sean especificaciones de hardware, de software, de licenciamiento. • Pruebas de laboratorio, que certifiquen el procedimiento de implementación y las funcionalidades técnicas del producto. • Instalación y configuración de la solución. • Pruebas de la solución implementada. • Elaboración de la documentación de la solución implementada. • 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 • Otros requerimientos asignados por el Jefe de Proyecto.

		que compone el Ítem paquete 01 o documento equivalente emitido por el fabricante que acredite que el personal cuenta con los conocimientos necesarios para realizar implementaciones en el componente/solución de Software de gestión de identidades, provisionamiento y roles. No se aceptará certificaciones de venta o pre venta. • Experiencia mínima de tres (03) años en servicios de implementación o soporte en soluciones de seguridad informática.	
1	Implementador II	• 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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en el componente/solución de Software de autenticación Multifactor que compone el Ítem paquete 01 No se aceptará certificaciones de venta o pre venta.	• Levantamiento de información de la infraestructura del MEF. • Apoyo en la instalación y configuración de la solución ofertada. • Apoyo en la elaboración de la documentación de la solución implementada. • 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. • Otros requerimientos asignados por el Jefe de Proyecto.

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:

ITEM PAQUETE 01

Ítem Paquete 01		
Solución de Gestión de Identidades		
Prestación	**Descripción**	**Cantidad**
Principal	Software de gestión de identidades, provisionamiento y roles	1
	Software de autenticación Multifactor	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	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 disgregada 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 cada paquete.

15.1 Cumplimiento 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 de la prestación 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.

15.2 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 perdida 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.

15.3 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.

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 Secretaria General N° 007-2014-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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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, enlaces web, 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, 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.
- ✓ Documentación donde se indique de manera detallada el peso (kg), espacio (m2), disipación de energía (BTU/hr) y energía eléctrica (watts), de cada uno de los equipos ofertados según corresponda.
- ✓ 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 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° 972-2020-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

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

El plazo máximo de entrega de los bienes de la prestación principal, de las soluciones que se detallan en el Anexo A1 es de cincuenta (50) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

Plazo de implementación

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

20. 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.

Para el ítem paquete 01 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, sitio en Jr. Jr. Lampa N° 274 - Cercado de Lima, 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.
- Actividades a realizar.
- 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.
- Hitos de implementación.
- Diagrama Gantt (Cronograma)
- Horarios de trabajo
- Configuraciones propuestas en las soluciones ofertadas.
- Procedimientos de inspección.
- Documentación del personal responsable para las coordinaciones administrativas para llevar el control sobre la prestación accesoria.
- Documentación del personal propuesto que brindará la asistencia técnica de la prestación accesoria y deberá contar como mínimo con el perfil y experiencia solicitada.
- Responsabilidades y consideraciones.
- Análisis y gestión de riesgos
    - Identificación de riesgos
    - Valoración de riesgos
    - Controles a implementar

- Plan de vuelta atrás
- Carta del fabricante que indique lo solicitado en el numeral 2.3 del Anexo A3 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 cincuenta (50) 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, sitio en Jr. Lampa N° 274 - Cercado de Lima.

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 implementación de la prestación principal, se deberá entregar un Informe Final, a través de mesa de parles del Ministerio, sitio en Jr. Lampa N° 274 - Cercado de Lima, 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 lógicos implementados.
- Respaldo de las configuraciones realizadas en toda la solución ofertada.
- Documento descriptivo de configuraciones de toda la solución ofertada.
- 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.
- Informe de verificación de cumplimiento de todos los requerimientos técnicos de las presentes especificaciones técnicas
- Informe de Conclusiones y Recomendaciones.

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.

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.

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 aplicara las siguientes multas, de acuerdo con lo dispuesto por el artículo 161° y 163º del reglamento de la Ley de Contrataciones del Estado. La acumulación de multas 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	Incumplimiento de programa o ejecución de trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	Por incumplimiento de participación del personal Cuando se detecte que EL CONTRATISTA envía a un personal clave 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.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 multa, la falta continúa, se volverá a aplicar la sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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.
5	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

ITEM PAQUETE 01

Ítem Paquete 01	
Anexo A1	Características técnicas de la solución de Gestión de Identidades
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 01, se debe considerar lo siguiente:

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 3´000,000.00 (Tres 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 autenticación Multifactor.
- Venta o Adquisición de solución de Gestión de identidades.
- Venta o Adquisición de certificados digitales SSL para aplicativos.
- Venta o Adquisición de certificados digitales.
- 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 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.

Acreditación para el Ítem Paquete 01:

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 01:

Requisitito
Coordinador
Experiencia mínima de tres (03) años en servicios de implementación o soporte o proyectos en soluciones de seguridad informática.

Implementador I
Experiencia mínima de tres (03) años en servicios de implementación 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 DE GESTIÓN DE IDENTIDADES

A. Software de gestión de identidades, provisionamiento y roles

I. Características Generales

1. Debe estar licenciada para 2500 usuarios por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe tener una función de creación de identidad en ausencia de una fuente autorizada (por ejemplo, terceros).
3. Debe tener métodos para la integración con sistemas externos, como los sistemas de Service Desk, a través de los servicios web.
4. Debe permitir que se creen atributos adicionales directamente a través de la herramienta.
5. Debe poder crear atributos de las aplicaciones y fuentes de datos, así como ser gestionados internamente por la herramienta.
6. Debe ser capaz de crear, cambiar y eliminar cuentas de usuario en sistemas integrados.
7. Debe permitir la creación de informes personalizados.
8. Debe permitir la creación de informes gráficos y paneles de control.
9. Debe permitir la programación de informes.
10. Debe permitir informes automáticos por correo electrónico.
11. Debe permitir la configuración de informes y paneles desde la interfaz web.
12. Debe permitir la exportación de los informes en formatos como PDF, Excel y archivo CSV.
13. Debe tener una integración nativa con herramientas de gestión de datos no estructurados y acceso privilegiado.
14. Debe proveer un portal de autoservicio para el reseteo de contraseñas de usuario. Este debe ser personalizable y en idioma español.
15. Debe soportar y ser compatible con el protocolo IPv6.
16. Debe administrarse a través de la interfaz web, sin la necesidad de instalar "clientes".
17. Debe admitir una comunicación segura entre los componentes.
18. Debe tener pistas de auditoría sobre las acciones tomadas.
19. Debe permitir la creación de diferentes perfiles de acceso para la administración de la herramienta en sí.
20. Debe tener integración con herramientas de correo electrónico para enviar notificaciones, aprobaciones.
21. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.

II. Gobierno

1. Debe tener la capacidad de recopilar datos de fuentes y aplicaciones autorizadas sin instalar agentes.
2. Debe tener un mecanismo que detenga la recopilación de datos si la fuente tuvo un porcentaje de cambios.
3. Debe admitir múltiples fuentes autorizadas para construir la identidad del usuario.
4. Debe poder identificar los cambios realizados directamente en las aplicaciones integradas.
5. Debe poder identificar cuentas de usuario que no se correlacionan con ninguna identidad (cuentas huérfanas).
6. Debe poder correlacionar las cuentas e identidades de los usuarios utilizando cualquier atributo de cuenta o de identidad.
7. Debe permitir la asociación de una cuenta a una identidad.

8. Debe poder recopilar información como: identidades, cuentas, perfiles, derechos
9. Debe poder programar colecciones.
10. Debe permitir que se creen filtros para la recopilación de datos.
11. Debe permitir que ciertas cuentas del sistema se clasifiquen como cuentas privilegiadas o cuentas de servicio.
12. Debe admitir la creación de descripciones fáciles de usar para los permisos de las aplicaciones integradas.
13. Debe poder crear reglas de segregación de funciones basadas en cualquier tipo de acceso presente en el sistema.
14. Debe poder verificar las reglas de segregación de funciones en los subcomponentes de un perfil.
15. Debe permitir que el jefe del usuario analice las violaciones de segregación de funciones o deberá permitir usuarios y grupos, y el usuario administrador de la plataforma deberá poder analizar las violaciones de segregación de funciones.
16. Debe permitir un acceso excepcional (violaciones aprobadas).
17. Debe permitir una justificación de negocio y una fecha de vencimiento para un acceso excepcional.
18. Debe permitir que se indique un control compensatorio para un acceso excepcional.
19. Debe permitir la importación de una matriz de segregación de funciones existente en la empresa.
20. Debe permitir que una regla de segregación tenga acceso a diferentes aplicaciones en su composición.
21. Debe poder realizar revisiones de acceso basadas en el usuario, así como perfiles de usuario.
22. Debe ser capaz de mostrar la descripción general de la certificación de acceso.
23. Debe permitir que las revisiones de acceso se realicen a través de la interfaz web.
24. Debe poder mostrar cualquier infracción de acceso durante las campañas de revisión.
25. Debe permitir que las revisiones de acceso se restrinjan a un grupo de usuarios en particular o acceso de acuerdo con los filtros de atributos.
26. Debe permitir que se inicie una revisión de acceso dado un cambio de usuario, como un cambio de departamento.
27. Debe permitir que las revisiones de acceso sean delegadas a otros por el revisor original.
28. Debe proporcionar el historial de revisiones de acceso para el revisor actual.
29. Debe proporcionar un análisis durante la revisión de acceso, por ejemplo:
    - Común
    - No común
    - Excepcional
    - Privilegiado
    - Violaciones o determinaciones de revisión de acceso mediante un scoring de riesgo.
30. Debe poder notificar automáticamente a los revisores cuando comience una nueva campaña de revisión.
31. Debe permitir una revisión de acceso de dos personas, revisión de múltiples pasos.

32. Debe permitir que la campaña de revisión realice de forma programa y contenga elementos que nunca han sido revisados o revisados previamente en un número determinado de meses.
33. Debe permitir que un revisor personalice la vista de revisión reordenando, eliminando o agregando campos.
34. Debe permitir la creación de revisiones de acceso que tengan violaciones de políticas.
35. Debe permitir que las campañas de revisión se programen para iniciarse automáticamente.

III. Ciclo de Vida

1. Debe permitir la sincronización bidireccional de los atributos integrados de la aplicación.
2. Debe tener al menos los siguientes conectores nativos: LDAP, Base de datos, Servicios web (SOAP y RESTful).
3. Debe permitir la creación de conectores personalizados.
4. Debe permitir que las contraseñas utilizadas en los conectores se almacenen en un Password Vault fuera de la herramienta.
5. Debe poder agregar accesos asignados a un nuevo usuario que se haya importado de la fuente autorizada.
6. Debe poder modificar el acceso de un usuario cuando sufre un cambio mapeado en la fuente autorizada.
7. Debe poder eliminar todos los accesos de un usuario cuando el usuario está inactivo en la fuente autorizada.
8. Deber permitir la creación de conectores a través de la interfaz web sin la necesidad de desarrollar código.
9. Deber permitir el aprovisionamiento manual en los casos en que no sea posible el aprovisionamiento automático.
10. Debe permitir que las acciones del conector se prueben por separado del flujo de aprovisionamiento.
11. Debe permitir la exportación/importación del conector.
12. Deber permitir que los flujos de trabajo se configuren a través de la interfaz web.
13. Debe permitir la aprobación respondiendo al correo electrónico de aprobación enviado por el sistema.
14. Debe tener la capacidad de establecer escalamientos de aprobación.
15. Debe admitir la configuración de aprobación dinámica basada en los atributos del usuario, el acceso que se otorgará y el propietario de la aplicación.
16. Debe tener la capacidad de asignar aprobadores temporales durante la ausencia del aprobador primario.
17. Debe tener la capacidad de ver todas las solicitudes pendientes.
18. Debe permitir al aprobador: aprobar completamente una solicitud, aprobar parcialmente la solicitud (rechazar cierto acceso que se ha solicitado), rechazar la solicitud por completo, asignar la aprobación a otra persona y devolver la solicitud para que el solicitante agregue más información.
19. Deber permitir la consulta con sistemas externos a través de WebServices durante Workflow.
20. Debe permitir el registro del propietario para diferentes objetos del sistema, como aplicaciones, perfiles, reglas, etc.
21. Debe permitir la inclusión de múltiples niveles de aprobación en un flujo de trabajo, ya sea en forma paralela o secuencial.
22. Debe permitir la solicitud de acceso temporal, con fecha de inicio y fecha de vencimiento de acceso.

23. Debe permitir que la solicitud de ciertos accesos se restrinja a grupos de usuarios en función de sus atributos.
24. Debe permitir que ciertas solicitudes de acceso se realicen solo a través de perfiles técnicos, por ejemplo.
25. Debería poder sugerir el acceso del solicitante en función de sus atributos.
26. Debe poder mostrar al usuario final el acceso que ya tiene.
27. Debe poder mostrar la violación de una regla de segregación de roles al otorgar y aprobar un acceso.

IV. Perfiles de acceso

1. Debe permitir la creación de al menos perfiles de acceso técnico y no técnico.
2. Debe tener la capacidad de realizar "Minería de roles" para definir los perfiles de acceso.
3. Debe permitir que los perfiles creados tengan reglas automáticas de asociación de usuarios.
4. Debe poder asociar/eliminar un perfil con un usuario cambiando uno o más atributos en la fuente autorizada.
5. Debe ser capaz de advertir sobre infracciones de acceso al cambiar un perfil.
6. Debe permitir la jerarquía de perfiles (uno o más perfiles técnicos dentro de un perfil empresarial, por ejemplo).
7. Debe tener un mecanismo que ayude a identificar el acceso y los usuarios faltantes o excedentes en un perfil.

V. Gestión de contraseñas

1. Debe admitir la creación de múltiples políticas de contraseña que pueden asociarse con una o más aplicaciones.
2. Debe admitir la recuperación de contraseña a través de preguntas de seguridad.
3. Debe permitir que las contraseñas generadas por el sistema se vean de forma segura.
4. Debe admitir la sincronización de la contraseña de la aplicación asociada con la misma política de contraseña y/o política general de contraseña (metadirecto) que sea abarcativa de todas las políticas individuales de cada aplicación.
5. Debe permitir a los usuarios finales cambiar las contraseñas de las aplicaciones integradas.
6. Debe poseer una interface autoservicio para la recuperación de contraseñas.

B. Software de Autenticación de Multifactor

1. Debe estar licenciada para 2500 usuarios por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe incluir como mínimo las siguientes autenticaciones:
   I. Software Token.
   II. Notificación Push.
   III. Reconocimiento facial.
3. Debe ser compatible con la autenticación multifactor.
4. Debe admitir Token de hardware como factor de autenticación.
5. Debe admitir Token Software como factor de autenticación.
6. Debe admitir "Notificación push" como factor de autenticación.
7. Debe admitir la biometría de dispositivos celulares como factor de autenticación.

8. Debe admitir al menos los sistemas operativos Windows, MacOS, Android e iOS para instalar autenticadores.
9. Debe admitir el token FIDO como factor de autenticación.
10. Debe admitir controles de autenticación basada en direcciones IP.
11. Debe admitir control de autenticación basado en tiempo y geolocalización para determinar si una persona inicio sesión en zonas físicas lejanas.
12. Debe ser compatible con el envío de una contraseña única (OTP) a través de SMS.
13. Debe admitir el envío de una contraseña de un solo uso (OTP) por correo electrónico.
14. Debe tener autenticación de autoservicio para el registro del autenticador.
15. Debe permitir operaciones masivas (asociación de tokens, distribución de tokens, etc.).
16. Debe admitir la distribución segura de tokens (descarga de semillas por autenticador y no solo envío de semillas).
17. Debe admitir métodos de autenticación para acceso de emergencia (problemas de autenticación).
18. Debe permitir la autenticación offline del Software Token (en los casos en que el dispositivo que aloja el Software Token no tiene conectividad).
19. Se requiere que la solución a ofertar se integre con la solución de ClearPass (Aruba). Los mecanismos de integración a utilizar serán las que ambas tecnologías mencionadas puedan soportar.
20. Debe contar con una interface de administración web.
21. Todos los componentes necesarios a fin de cumplir con los requerimientos técnicos deben ser provistos como parte de la solución.

I. SSO

1. Debe admitir el ingreso de inicio de sesión único (SSO) para aplicaciones web.
2. Debe admitir el uso de servidores LDAP como fuente de identidad de autenticación.
3. Debe admitir la federación de identidad, como el proveedor de identidad y el proveedor de servicios.
4. Debe permitir la integración con aplicaciones web a través de Reverse Proxy y encabezados HTTP.
5. Debe permitir como mínimo la integración con aplicaciones a través de RADIUS y/o form fill y/o HTTP header y/o Identity Injection y/o un conector a medida.
6. Debe permitir la autenticación a través de las API RESTful.
7. Debe permitir la autenticación integrada de Windows.
8. Debe tener un portal de inicio de sesión único, donde estén disponibles los enlaces de las aplicaciones a las que el usuario tiene acceso.
9. Debe permitir al usuario marcar un navegador como confiable (opcional)
10. Debe admitir reglas de acceso autoritativas basadas en atributos de origen autoritativos.
11. Debe admitir la creación de reglas de acceso basadas en IP de origen.
12. Debe admitir el uso de "navegador de confianza" dentro de una regla de acceso (opcional)
13. Debe proporcionar análisis de riesgos basados en el comportamiento, el dispositivo y la ubicación.
14. Debe admitir listas negras de usuarios dentro de sus reglas de acceso.

ANEXO A2

SOLUCIÓN DE GESTIÓN DE IDENTIDADES

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

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 solución.

B. Instalación y configuración

1. Se debe implementar la plataforma en los servidores del ambiente virtual del Ministerio.
2. La solución deberá ser instalada en todos los equipos indicados por la entidad. Los dispositivos están distribuidos en Lima y provincias, pudiendo realizar la instalación del software de forma remota. En caso de no funcionar deberá ser de manera presencial.
3. 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.
4. La solución ofertada debe ser configurada para que trabaje en un esquema de alta disponibilidad entre el centro de datos principal, contingencia y recuperación de desastres.
5. Se debe crear como mínimo un usuario por cada rol existente en la plataforma.
6. Se debe configurar cada componente de autenticación para estar activo y para ser consumido.
7. Se debe realizar otras configuraciones que el implementador considere necesario para el correcto funcionamiento de la plataforma.
8. Se debe integrar la solución al Directorio Activo.
9. Se debe integrar la solución para cinco (05) aplicaciones (Clearpass, Oracle, MySQL, SQLServer, MySQL). El cuadro de roles se proporcionará durante el levantamiento de la información.
10. Se debe realizar un afinamiento según las buenas prácticas recomendadas por el fabricante de la plataforma.
11. 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:
    - ✓ 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

SOLUCIÓN DE GESTIÓN DE IDENTIDADES

CONTRATACIÓN DEL SERVICIO DE CONTINUIDAD OPERATIVA

1. Consideraciones generales

- Este servicio cubrirá todo el hardware y 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.
- La asistencia técnica necesaria será brindada por personal técnico calificado y especializado en los productos ofrecidos, quien deberá estar debidamente capacitado para dicha labor.
- Las labores técnicas a realizar sobre la solución se llevarán a cabo en el lugar donde éstos se encuentren instalados.
- 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.
- 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, por vía telefónica o por mensajería instantánea. 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 el registro o reportes de incidentes, fallas, problemas y requerimientos, según corresponda, así como también realizar el seguimiento, monitoreo de estado de los componentes de la solución, 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 trabajo, 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.
- Se deberá asignar a un especialista como "Personal Residente" en las instalaciones del Ministerio en el horario de oficina (de lunes a viernes de 9:00 a 18:00 horas) a fin de monitorear la solución ofertada y realizar las configuraciones que hubiese, por el periodo de mil noventa y cinco (1095) días calendario, que iniciaran una vez firmada la conformidad de la prestación principal. Previa coordinación con el personal de la OGTI del MEF se prestarán los servicios de manera remota.
- 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.
- 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 revisar y evaluar el estado de la solución materia del presente contrato. El contratista, de detectar un imperfecto o anomalía deberá realizar cualquier ajuste necesario para su corrección.
- 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. 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 ser brindada dentro de los primeros noventa (90) días calendario del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- Debe estar enfocada en las funcionalidades a nivel de administración de todas las soluciones ofertada.
- 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 uno de las personas debe recibir una capacitación mínima de cuarenta (40) horas por cada una de las dos (2) soluciones que componen el ítem paquete 01. Se aceptará un workshop adicional para completar la cantidad de horas solicitadas para la capacitación oficial, solo en casa 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 (fuera del horario de oficina) y sábados.

2.3.1. 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.

2.3.2. 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, 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.

2.4. 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.

2.4.1. 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.

2.4.2. 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 del 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.

2.4.3. Servicio de Capacitación

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 capacitación, según detalle:

- Documento de Capacitación.
  - Nombre del personal
  - Temario
  - Cantidad de horas de la capacitación brindada.
  - Certificados de los participantes de la capacitación.

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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Incidencias Corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo en la solución	**Alto**	**Tiempo de respuesta:** 30 minutos **Tiempo de solución:** 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.
	Medio	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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.
	Bajo	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Requerimiento Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	**Medio**	**Tiempo de Respuesta** 2 horas **Tiempo de Solución** 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.

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 I o implementador II 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. 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.

Personal de capacitación: Será la persona encargada de brindar la capacitación en el manejo de la solución ofertada al personal designado por la OIT.
El personal para la capacitación debe estar avalado por la marca para brindar la capacitación oficial.

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	Incumplimiento De Programa O Ejecución De Trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	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 del servicio (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 multa, la falta continúa, se volverá a aplicar la sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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
5	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:

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

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:

THM = 24 x 90 = 2,160 horas

THE = 4+3 = 7 horas

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

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%

Rango de UPTIME	Penalidad(1)
>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 calendario, 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 Tecnología 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 Capacitación, se realizará un solo pago, luego de emitida la conformidad, previa presentación del Documento de Capacitación.
- 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.

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 perdida 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 Secretaria 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 dictadas 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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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

1. 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.

ANEXO A4

Solución de Gestión de Identidades

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.**
A. Software de gestión de identidades, provisionamiento y roles					
I. Características generales					
1. Debe tener una función de creación de identidad en ausencia de una fuente autorizada (por ejemplo, terceros).					
2. Debe tener métodos para la integración con sistemas externos, como los sistemas de Service Desk, a través de los servicios web.					
3. Debe permitir que se creen atributos adicionales directamente a través de la herramienta.					
4. Debe poder crear atributos de las aplicaciones y fuentes de datos, así como ser gestionados internamente por la herramienta.					
5. Debe ser capaz de crear, cambiar y eliminar cuentas de usuario en sistemas integrados.					
6. Debe permitir la creación de informes personalizados.					
7. Debe permitir la creación de informes gráficos y paneles de control.					
8. Debe permitir la programación de informes.					
9. Debe permitir informes automáticos por correo electrónico.					
10. Debe permitir la configuración de informes y paneles desde la interfaz web.					
11. Debe permitir la exportación de los informes en formatos como PDF, Excel y archivo CSV.					
12. Debe tener una integración nativa con herramientas de gestión de datos no estructurados y acceso privilegiado.					

13. Debe proveer un portal de autoservicio para el reseteo de contraseñas de usuario. Este debe ser personalizable y en idioma español.				
14. Debe soportar y ser compatible con el protocolo IPv6.				
15. Debe administrarse a través de la interfaz web, sin la necesidad de instalar "clientes".				
II. **Gobierno**				
1. Debe tener la capacidad de recopilar datos de fuentes y aplicaciones autorizadas sin instalar agentes.				
2. Debe tener un mecanismo que detenga la recopilación de datos si la fuente tuvo un porcentaje de cambios.				
3. Debe admitir múltiples fuentes autorizadas para construir la identidad del usuario.				
4. Debe poder identificar los cambios realizados directamente en las aplicaciones integradas.				
5. Debe poder identificar cuentas de usuario que no se correlacionan con ninguna identidad (cuentas huérfanas).				
6. Debe poder correlacionar las cuentas e identidades de los usuarios utilizando cualquier atributo de cuenta o de identidad.				
7. Debe permitir la asociación de una cuenta a una identidad.				
8. Debe poder recopilar información como: identidades, cuentas, perfiles, derechos				
9. Debe poder programar colecciones.				
10. Debe permitir que se creen filtros para la recopilación de datos.				
11. Debe ser capaz de mostrar la descripción general de la certificación de acceso.				
12. Debe permitir que las revisiones de acceso se realicen a través de la interfaz web.				
13. Debe poder mostrar cualquier infracción de acceso durante las campañas de revisión.				
14. Debe permitir que las revisiones de acceso se restrinjan a un grupo de usuarios en particular o acceso de acuerdo con los filtros de atributos.				
15. Debe permitir que se inicie una revisión de acceso dado un cambio de usuario, como un cambio de departamento.				
16. Debe permitir que las revisiones de acceso sean delegadas a otros por el revisor original.				
III. Ciclo de Vida				

1. Debe permitir la sincronización bidireccional de los atributos integrados de la aplicación.				
2. Debe tener al menos los siguientes conectores nativos: LDAP, Base de datos, Servicios web (SOAP y RESTful).				
3. Debe permitir la creación de conectores personalizados.				
4. Debe permitir que las contraseñas utilizadas en los conectores se almacenen en un Password Vault fuera de la herramienta.				
5. Debe poder agregar accesos asignados a un nuevo usuario que se haya importado de la fuente autorizada.				
6. Debe permitir el registro del propietario para diferentes objetos del sistema, como aplicaciones, perfiles, reglas, etc.				
7. Debe permitir la inclusión de múltiples niveles de aprobación en un flujo de trabajo, ya sea en forma paralela o secuencial.				
8. Debe permitir la solicitud de acceso temporal, con fecha de inicio y fecha de vencimiento de acceso.				
9. Debe permitir que la solicitud de ciertos accesos se restrinja a grupos de usuarios en función de sus atributos.				
IV. Perfiles de acceso				
1. Debe tener la capacidad de realizar "Minería de roles" para definir los perfiles de acceso.				
2. Debe permitir que los perfiles creados tengan reglas automáticas de asociación de usuarios.				
3. Debe poder asociar/eliminar un perfil con un usuario cambiando uno o más atributos en la fuente autorizada.				
4. Debe ser capaz de advertir sobre infracciones de acceso al cambiar un perfil.				
5. Debe permitir la jerarquía de perfiles (uno o más perfiles técnicos dentro de un perfil empresarial, por ejemplo).				
6. Debe tener un mecanismo que ayude a identificar el acceso y los usuarios faltantes o excedentes en un perfil.				
V. **Gestión de contraseñas**				
1. Debe admitir la creación de múltiples políticas de contraseña que pueden asociarse con una o más aplicaciones.				
2. Debe admitir la recuperación de contraseña a través de preguntas de seguridad.				
3. Debe permitir que las contraseñas generadas por el sistema se vean de forma segura.				

B. Software de Autenticación de Multifactor				
1. Debe incluir las siguientes autenticaciones: • Software Token. • Notificación Push. • Reconocimiento facial.				
2. Debe ser compatible con la autenticación multifactor.				
3. Debe admitir Token de hardware como factor de autenticación.				
4. Debe admitir Token Software como factor de autenticación.				
5. Debe admitir "Notificación push" como factor de autenticación.				
6. Debe admitir la biometría de dispositivos celulares como factor de autenticación.				
7. Debe admitir controles de autenticación basada en direcciones IP.				
8. Debe admitir control de autenticación basado en tiempo y geolocalización para determinar si una persona inicio sesión en zonas físicas lejanas.				
9. Debe ser compatible con el envío de una contraseña única (OTP) a través de SMS.				
10. Debe admitir el envío de una contraseña de un solo uso (OTP) por correo electrónico.				
11. Debe tener autenticación de autoservicio para el registro del autenticador.				
12. Debe permitir operaciones masivas (asociación de tokens, distribución de tokens, etc.).				
13. Debe admitir la distribución segura de tokens (descarga de semillas por autenticador y no solo envío de semillas).				
I. **SSO**				
1. Debe admitir el ingreso de inicio de sesión único (SSO) para aplicaciones web.				
2. Debe admitir el uso de servidores LDAP como fuente de identidad de autenticación.				
3. Debe admitir la federación de identidad, como el proveedor de identidad y el proveedor de servicios.				
4. Debe permitir la integración con aplicaciones web a través de Reverse Proxy y encabezados HTTP.				
5. Debe permitir como mínimo la integración con aplicaciones a través de RADIUS y/o form fill y/o HTTP header y/o Identity Injection y/o un conector a medida				
6. Debe permitir la autenticación a través de las API RESTful.				

ITEM PAQUETE 02

CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.

ESPECIFICACIONES TÉCNICAS
CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES 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 protección de ambientes virtuales 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 protección de ambientes virtuales 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 evolución acelerada de los ataques cibernéticos requiere una implementación de nuevos componentes tecnológicos de protección que permitan hacer frente a las nuevas amenazas cibernéticas orientadas específicamente a los servicios tecnológicos que ofrece el MEF a sus distintos usuarios internos y externos.

5. Objetivo De La Contratación

5.1. Objetivo General

Implementar soluciones para la mejora de la protección ambientes virtuales de la Infraestructura Tecnológica del MEF.

5.2. Objetivo Específico

- ✓ Establecer protección para los ambientes virtuales.

6. Alcance y descripción de los bienes a contratar

6.1. Descripción y cantidad de los bienes

La presente adquisición está compuesta por los siguientes bienes a contratar, los mismos que se describe en el siguiente cuadro:

ITEM PAQUETE 02

Ítem Paquete 02		
Soluciones para la protección de ambientes virtuales		
Prestación	**Descripción**	**Cantidad**
Principal	Solución para la Protección de Ambientes SDDC (Software Defined Data Center) - Next Generation Firewall para Vmware NSX de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente[1]	1
	Solución para la Protección de Contenedores y Gestor de Contenedores - Prisma Cloud Compute de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente[2]	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

6.2. Distribución de las soluciones

Distribución de las soluciones teniendo en cuenta su ubicación:

Ítem Paquete 02

Solución para la Protección de Ambientes SDDC (Software Defined Data Center) - Next Generation Firewall para Vmware NSX de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente.

- La solución deberá estar implementado en los centros de datos Principal, Contingencia y Recuperación de Desastres.

Solución para la Protección de Contenedores y Gestor de Contenedores - Prisma Cloud Compute de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente.

- La solución deberá estar implementado en los centros de datos Principal, Contingencia y Recuperación de Desastres.

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 ciberseguridad para la protección de ambientes virtuales 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 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

[1] Informe Técnico de Estandarización N° 006-2021-EF/OGTI, aprobado mediante Resolución Directoral N° 128-2021-EF43.01

[2] Informe Técnico de Estandarización N° 006-2021-EF/OGTI, aprobado mediante Resolución Directoral N° 128-2021-EF43.01

tampoco deberá crear inconvenientes de disponibilidad a las aplicaciones existentes.

- ✓ La solución deberá ser ofrecida en su versión más estable y/o avanzada El contratista deberá ofertar la última versión disponible del Hardware y Software del fabricante. 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.
- ✓ Todos los equipos deben ser nuevos, sin uso y de reciente fabricación. No se aceptarán equipos usados o re manufacturados.
- ✓ 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, para la cual 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 la 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 software requeridos en el **ANEXO A1** mismo que debe cumplir como mínimo con las siguientes características técnicas:

ITEM PAQUETE 02

Soluciones para la protección de ambientes virtuales	
Descripción	Anexo
Características técnicas de las soluciones para la protección de ambientes virtuales	A1

7.2.2. Implementación: Levantamiento de información, instalación, configuración, pruebas y puesta en marcha**.**

El Contratista deberá implementar el equipamiento de hardware y software 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 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 todos los servidores y herramientas proporcionadas (Hardware y Software), todo el cableado y su etiquetado (energía, redes), los switch.
- ✓ Los requerimientos específicos del ítem paquete 02 se detalla en el anexo A2.

ITEM PAQUETE 02

Ítem Paquete 02	
Soluciones para la protección de ambientes virtuales	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	A2

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 emitida la Conformidad de la Prestación Principal. Esta garantía debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 del día siguiente de emitida la Conformidad de la Prestación Principal. Esto debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 equipamiento o hasta que se encuentren vigentes por el fabricante.
- ✓ La garantía de los equipos suministrados será por un período de mil noventa y cinco (1095) días calendario, contado a partir del día siguiente de emitida la Conformidad, 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.

- ✓ Todos los componentes de la Plataforma Tecnológica propuesta no podrán presentar adulteraciones ni correcciones (por ejemplo: tarjeta madre, fuente, etc.).

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 Accesoria a los bienes ofertados en la Prestación Principal (Anexo A1)

Los requerimientos específicos por ítem paquete 02 se detalla en el anexo A3.

ITEM PAQUETE 02

Ítem Paquete 02	
Soluciones para la protección de ambientes virtuales	
Descripción	Anexo
Servicio de continuidad operativa	A3

12. FUNCIONES DEL PERSONAL

Se detalla las funciones del personal:

ITEM PAQUETE 02

Ítem Paquete 02			
Soluciones para la protección de ambientes virtuales			
Cant.	Personal	Perfil	Actividades
1	Coordinador (Personal Clave)	• Titulado en Administración o Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería electrónica o Ingeniería de las telecomunicaciones o Ingeniería de Computación y Sistemas. • Certificación de PMP (Project Management Professional). • Experiencia mínima de tres (03) años en servicios de implementación o soporte en el producto ofertado del personal clave requerido como Coordinador.	• Coordinar la implementación de la solución. • Coordinar con el encargado del área de la OGTI del MEF. • Coordinar con los implementadores de su empresa para el cumplimiento de los objetivos en el tiempo planificado. • Reportar a la OGTI los avances según el cronograma establecido en el plan de trabajo. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana).
1	Implementador I (Personal Clave)	• Bachiller en Ingeniería de Sistemas o Sistemas y Computación o Sistemas y Telecomunicaciones o	• Análisis de los detalles técnicos de la tecnología que se va implementar, ya sean especificaciones de hardware, de software, de licenciamiento.

		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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en la solución ofertada, Se aceptará certificado oficial de las marcas que conformen la solución. No se aceptará certificaciones de venta o pre venta. • Experiencia mínima de tres (03) años en servicios de implementación o soporte en el producto ofertado del personal clave requerido como Implementador I.	• Pruebas de laboratorio, que certifiquen el procedimiento de implementación y las funcionalidades técnicas del producto. • Instalación y configuración de la solución. • Pruebas de la solución implementada. • Elaboración de la documentación de la solución implementada. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). • Otros requerimientos asignados por el Jefe de Proyecto.
1	Implementador II	• 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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en la solución ofertada, Se aceptará certificado oficial de las marcas que conformen la solución. No se aceptará certificaciones de venta o pre venta.	• Levantamiento de información de la infraestructura del MEF. • Apoyo en la instalación y configuración de la solución ofertada. • Apoyo en la elaboración de la documentación de la solución implementada. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). • Otros requerimientos asignados por el Jefe de Proyecto.

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

ITEM PAQUETE 02

Ítem Paquete 02		
Soluciones para la protección de ambientes virtuales		
Prestación	**Descripción**	**Cantidad**
Principal	Solución para la Protección de Ambientes SDDC (Software Defined Data Center) - Next Generation Firewall para Vmware NSX de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente	1
	Solución para la Protección de Contenedores y Gestor de Contenedores - Prisma Cloud Compute de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

Por motivo que los bienes y servicios se encuentran relacionados entre sí, se considera conveniente realizar contrataciones 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 disgregada 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 cada paquete.

15.1. Cumplimiento 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 de la prestación 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.

15.2. 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 perdida 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.

15.3. 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. El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria General N° 007-2014-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.

Las adecuación e 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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías o moleculares para COVID-19 es potestativo, salvo que el Ministerio identifique un caso sospechoso del personal propuesto, en tal sentido se autorizara el cambio del personal, luego del reporte del área usuaria de la Entidad.

17. Otros documentos

17.1. Para la presentación de oferta

- ✓ Los postores deberán presentar la siguiente documentación: Folletos, brochures, certificados, enlaces web, 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, 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.
- ✓ Documentación donde se indique de manera detallada el peso (kg), espacio (m2), disipación de energía (BTU/hr) y energía eléctrica (watts), de cada uno de los equipos ofertados según corresponda.
- ✓ 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 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° 972-2020-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

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

El plazo máximo de entrega de los bienes de la prestación principal, de los equipos que se detalla en el Anexo A1 es de cincuenta (50) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

Plazo de implementación

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

20. 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.

Para el ítem paquete 02 se 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, sitio en Jr. Lampa N° 274 - Cercado de Lima, 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.
- Actividades a realizar.
- 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.
- Hitos de implementación.
- Diagrama Gantt (Cronograma)
- Horarios de trabajo
- Configuraciones propuestas en las soluciones ofertadas
- Procedimientos de inspección.

- Documentación del personal responsable para las coordinaciones administrativas para llevar el control sobre la prestación accesoria.
- 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 2.3 del Anexo A3 de corresponder.
- Responsabilidades y consideraciones.
- Análisis y gestión de riesgos
  - Identificación de riesgos
  - Valoración de riesgos
  - Controles a implementar
  - Plan de vuelta atrás

  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 cincuenta (50) 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, sitio en Jr. Lampa N° 274 - Cercado de Lima.

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 implementación de la prestación principal, se deberá entregar un Informe Final, a través de mesa de parles del Ministerio, sitio en Jr. Lampa N° 274 - Cercado de Lima, necesario para que se otorgue la conformidad de la Prestación Principal, donde se indique lo siguiente:

- Trabajos/actividades realizadas.
- Actas de avances de los trabajos (si las hubiese).

- Diagramas lógicos implementados.
- Respaldo de las configuraciones realizadas en todas las soluciones ofertadas en un dispositivo.
- Documento descriptivo de configuraciones de toda la solución ofertada.
- 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.
- Informe de Verificación de Cumplimiento de todos los requerimientos técnicos de las presentes especificaciones técnicas.
- Informe de Conclusiones y Recomendaciones

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.

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.

22. Adelantos

La entidad podrá otorgar un adelanto directo hasta por 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, adjuntando 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 aplicara las siguientes penalidades, de acuerdo con lo dispuesto por el artículo 161° y 163º 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	Incumplimiento de programa o ejecución de trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	Por incumplimiento de participación del personal Cuando se detecte que EL CONTRATISTA envía a un personal clave 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.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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.
5	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

ITEM PAQUETE 02

Ítem Paquete 02	
Anexo A1	Características técnicas de las soluciones para la protección de ambientes virtuales
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 02, se debe considerar lo siguiente:

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 5´000,000.00 (Cinco Millones con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran similares a los siguientes:

- Venta o Adquisición de solución de seguridad informática.
- Venta o Adquisición de equipamiento de seguridad perimetral.
- Venta o Adquisición de equipamiento de seguridad de TI.
- 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 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.

Acreditación para el ítem paquete 02:

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.

B. Capacidad técnica y profesional

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

Requisitito

Coordinador

Experiencia mínima de tres (03) años en servicios de implementación o soporte en el producto ofertado del personal clave requerido como **Coordinador.**

Implementador I
Experiencia mínima de tres (03) años en servicios de implementación o soporte o implementación de soluciones de seguridad informática en el producto ofertado del personal clave requerido como **Implementador I.**

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

SOLUCIONES PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES

I. Generalidades

1. Debe estar licenciada para 28 servidores físicos de virtualización master por un periodo de mil noventa y cinco (1095) días calendario.
2. Debe ser capaz de brindar seguridad a nivel de red de los servidores virtuales, microsegmentación a nivel de SDDC (Software Defined Data Center); contenedores, gestor, registros e imágenes de contenedores.
3. Deben ser ofrecida en dos plataformas de seguridad, una orientada a SDDC (Software Defined Data Center) y la otra orientada a Contenedores.
4. Las soluciones deben ser de propósito específico, no se aceptarán soluciones genéricas.

II. Solución para la Protección de Ambientes SDDC (Software Defined Data Center).

2.1. Generalidades

- Adquisición de una solución de tipo Next Generation Firewall (NGFW) para protección de redes de Data Center Definido por Software (SDDC) – **Next Generation Firewall para Vmware NSX** de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente.[3]
- El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.

2.2. Capacidades

- Cada equipo NGFW debe soportar 2 Gbps de throughput de Prevención de Amenazas (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, control de amenazas avanzadas de día cero (Sandboxing) y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección.
- Cada equipo NGFW debe soportar hasta 800 mil sesiones de conexiones simultaneas.
- Cada NGFW deberá requerir como máximo 100 GB para ser desplegados en el entorno virtual. Los recursos de hardware serán proporcionados por el MEF.

[3] Informe Técnico de Estandarización N° 006-2021-EF/OGTI, aprobado mediante Resolución Directoral N° 128-2021-EF43.01

2.3. Funcionalidades de Firewall

- Deberá integrarse de forma nativa con la solución de VMware NSX Manager versión 6.4 o superior, sin necesidad de hacer uso de software o plataformas terceras.
- Deberá integrarse de forma nativa con la solución de VMware NSX-T Manager versión 3.1 o superior, sin necesidad de hacer uso de software o plataformas terceras.
- Capacidad para desplegar los NGFW de manera automática (zero touch deployment) usando la integración con NSX Manager.
- No debe requerir cambios a nivel de la arquitectura de red VMware NSX
- Deberá tener visibilidad inmediata de los grupos de microsegmentación definidos en la plataforma de virtualización para poder establecer políticas de seguridad de capa 7 entre dichos microsegmentos.
- Debe permitir el redireccionamiento del tráfico entre los host o grupos de host de la plataforma virtual al NGFW de manera nativa y automática, para ello deberá estar integrado al hypervisor.
- Debe tener control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, usuarios y grupos de usuarios, aplicaciones grupos estáticos y dinámicos de aplicaciones.
- Debe permitir definir un grupo dinámico de IP, que se alimente de forma automática a través de la integración con VMware NSX.

2.4. Control de Aplicaciones

- Debe reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, bases de datos, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, storage, compartimiento de archivos, servicios de autenticación.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones, independientemente del puerto y protocolo que usen. Debe ser capaz de detectar si la aplicación esta usando o no su puerto estándar, por ejemplo, RDP por el puerto 80 en lugar del 3389.
- Para tráfico cifrado (SSL/TLS y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
- Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante.
- Debe contar con un módulo que se encargue de perfilar el tráfico de red e identifique las reglas de firewall que no cuenten con un control basado en aplicaciones, de tal forma que muestre que aplicaciones están pasando por una política de seguridad donde solo se han colocado puertos (capa 4) o no se ha definido ningún puerto ni aplicación.

2.5. Prevención de Amenazas

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Anti-malware de red), Antispyware o Antibot integrados en el propio appliance.
- Cuando se utilicen las funciones de Prevención de Amenazas el equipamiento debe entregar el mismo performance (no degradar) entre tener una única firma de seguridad habilitada o tener todas las firmas habilitadas.
- Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de

seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
- Debe ser capaz de inspeccionar malware que se propague por los protocolos HTTP, HTTP/2, HTTPS, FTP, SMB tanto en IPv4 como en IPv6.
- Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms. Esta funcionalidad también podrá ser cubierta con algún módulo que integre la prevención de amenazas desconocidas.
- Debe contar con firmas específicas para la mitigación de ataques DoS, buffer overflow, C2 (comando y control)
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

2.6. Control de Malware de Día Cero

- La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- Deberá soportar el análisis y emulación de malware en el Sandboxing en entornos Windows y Linux como mínimo.
- Debe soportar la inspección de archivos transferidos por los protocolos HTTP, HTTP/2, HTTPS, FTP, SMB, tanto en IPv4 como en IPv6.
- Deberá ofrecer un tiempo no mayor a 10 minutos, para la detección de malware de día cero.
- Deberá ser capaz de procesar al menos 1000 archivos por hora sin sufrir degradación ni encolamiento y haciendo uso completo de técnicas de emulación y análisis dinámico (es decir, sin considerar Firmas, ni Prefiltros de seguridad).
- El Sandboxing podrá ser ofrecido en modo Cloud o en modo Onpremise.
- En caso de que se oferte un Sandboxing Cloud, deberá garantizar la privacidad y seguridad de los datos analizados, por lo cual se requiere que cuente como mínimo con la certificación SOC2 Tipo 2 Plus de AICPA. El postor deberá adjuntar en su oferta la certificación o enlace de descarga oficial del fabricante. Asimismo, deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
- En caso de que se oferte un Sandboxing Onpremise, deberá ser desplegado en Alta Disponibilidad para mantener la redundancia del servicio.
- El sandbox debe proveer información sobre las acciones del malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el malware y generar firmas de antivirus automáticamente.
- El sandbox debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia interfaz de administración.
- El sandbox debe soportar, como mínimo, el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP y RAR) archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), flash en el ambiente controlado.
- El sandbox debe permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.

2.7. Plataforma de Gestión y Monitoreo

- La solución deberá contar con una consola de administración centralizada para la gestión y administración de todos los NGFW virtuales.
- La entidad brindará el entorno virtual incluyendo la licencia de software virtualización, así como también Licencia NSX, todo licenciamiento adicional

necesario para la implementación de la solución deberá ser proporcionado por el contratista.

- Debe soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
- Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
    - Mostrar la primera y última vez que se utilizó una regla de seguridad
    - Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.

III. Solución para la Protección de Contenedores y Gestor de Contenedores.

3.1. Generalidades

- Adquisición de una solución para la Protección de Contenedores y Gestor de Contenedores - **Prisma Cloud Compute** de la marca Palo Alto Networks (marca estandarizada por la Entidad), o equivalente.[4]
- Deberá consistir en una plataforma de protección de la carga de trabajo en la nube (CWPP: Cloud Workload Protection) proporcionando seguridad y protección de las cargas de trabajo en entornos de nube privada.
- La solución debe proteger automáticamente los contenedores, imágenes, registros, cargas de trabajo, aprendiendo sus características y comportamientos y aplicar políticas de seguridad en tiempo de ejecución o runtime.
- Debe ofrecer escalabilidad, incluyendo la capacidad de extender la protección hacia Nubes Públicas.
- La solución debe proteger un mínimo de 500 servidores que hostean contenedores.
- El gestor de contenedores del MEF está basado en Kubernetes.

3.2. Visibilidad en Nube

- La solución deberá proveer un CMDB (Base de datos de recursos y configuraciones) en consola gráfica y API
- Capacidad de monitoreo continuo en los entornos de nube privada para ayudar a garantizar que la infraestructura de nube esté protegida contra amenazas de seguridad.
- Deberá tener la capacidad de detección y respuesta de amenazas para configuraciones incorrectas de recursos y vulnerabilidades de los contenedores

[4] Informe Técnico de Estandarización N° 006-2021-EF/OGTI, aprobado mediante Resolución Directoral N° 128-2021-EF43.01

y proporcionar visibilidad de la actividad del usuario dentro de cada entorno de la nube privada.

3.3. Funcionalidades de Cumplimiento y Gobierno de Seguridad

- La solución debe monitorear continuamente los activos de nube y validar cumplimientos de normas de seguridad y estándares de cumplimiento de la industria
- La solución debe contener como mínimo los siguientes estándares de cumplimiento: CIS (Center for Internet Security) GDPR, HIPPA, NIST 800-190.
- Debería permitir la creación de nuevos estándares de cumplimiento personalizados, para reflejar los estándares de la organización.
- Los nuevos estándares de cumplimiento deben poder ser definidos en base a Contenedores, Imágenes, Hosts.
- Debe tener un panel de cumplimiento que muestre la postura de cumplimiento de los entornos de nube monitoreados con los diversos estándares existentes
- El escáner de imágenes debe buscas malware en binarios en las capas de imágenes, incluida la capa base.

3.4. Gestión de Vulnerabilidades

- Debe contar con un Dashboard que permita identificar las vulnerabilidades identificadas en los Contenedores, Registros, Imágenes, repositorios de código.
- Debe categorizar la criticidad de cada vulnerabilidad identificada y otorgar una puntuación de riesgo, que permita al administrador priorizar las vulnerabilidades a atender.
- Debe mostrar al menos la siguiente información de cada vulnerabilidad identificada: nivel de criticidad, complejidad y vector de ataque, disponibilidad del parche e identificación CVE.
- Deberá mostrar el repositorio de código y la ruta del archivo que presenta la vulnerabilidad, así como el registro y la imagen.
- Cada política debe permitir la definición de un nivel de severidad, disponibilidad de un parche, excepciones basadas en CVE, cluster, contenedor, imagen, namespace, repositorio de código.

3.5. Investigación de Incidentes

- Debe permitir la investigación de incidentes detectados mediante el análisis de la configuración de los recursos en la nube, consumiendo datos de configuración de las API de los servicios de las plataformas en la nube administradas.
- Debe permitir la investigación de incidentes detectados a través de registros de auditoría, consumiendo datos y eventos del usuario de los servicios de las plataformas de nube administradas, permitiendo la investigación de accesos de consola y API, el monitoreo de actividades privilegiadas y la detección compromisos de cuenta.
- Debe permitir la investigación de incidentes de red, consumir y monitorear el tráfico de red (flujos de tráfico) de servicios en la nube, permitiendo la consulta de eventos de red en plataformas de nube administradas. Debe detectar cuándo los servicios, aplicaciones o bases de datos están expuestos a Internet y si hay intentos potenciales de extraer datos
- Debe identificar cuándo las direcciones IP sospechosas acceden a los recursos monitoreados
- Debe ser posible configurar remediación automática para violaciones de políticas de seguridad

- Debe tener la capacidad de integración para enviar registros y alertas para herramientas SIEM e integración con herramientas de orquestación y automatización de respuesta a incidentes (SOAR)
- Debe admitir la integración con herramientas de tickets como ServiceNow, JIRA.
- Debe permitir enviar alertas por Correo, plataformas SOAR, Slack y ser personalizable con Webhook.

3.6. Capacidades de Detección y Protección

- Protección en runtime para sistemas operativos Linux, con control de aplicaciones, lista blanca y sistema de archivos;
- Debe permitir que la automatización y el aprendizaje automático modelen el comportamiento del proceso, red, sistema de archivos y llamadas al sistema, creando una lista de listas blancas de comportamiento, evitando comportamientos anómalos y ataques desconocidos. Por ejemplo, cuando se establece una conexión a red no esperada o cuando un contenedor se conecta a una Botnet
- Debe permitir la creación de reglas personalizadas;
- Debe tener protección en tiempo de ejecución mediante el aprendizaje automático (Machine Learning) para crear automáticamente un modelo de cada aplicación en el entorno.
- Los modelos de Machine Learning deben mapear y definir todos los comportamientos válidos de contenedores, a través de sensores de proceso, red, sistema de archivos y llamadas al sistema.
- La solución debe recopilar datos forenses de las cargas de trabajo, a medida que se ejecutan, antes de que ocurra un incidente.
- Debe tener una vista del estado de sus microservicios antes, durante y después de cualquier compromiso;
- Debe aprender automáticamente todos los registros y repositorios confiables para ejecutar las aplicaciones, lo que le permite asegurarse de que las imágenes se implementen solo desde esas fuentes confiables;
- La solución no debe insertar componentes como bibliotecas o agentes en los contenedores o imágenes;
- La solución debe soportar automáticamente el crecimiento del clúster, sin requerir intervención manual en el proceso de protección de nuevos nodos;
- La solución debe gestionar y evitar vulnerabilidades desde el desarrollo hasta la producción, integrándose con el proceso de CI (integración continua) a través de plug-ins o mediante la interfaz de línea de comandos (CLI), en el registro y en producción para identificar y priorizar vulnerabilidades y riesgos en contenedores, imágenes y registros.
- Debe permitir la creación de políticas personalizadas y automatizadas para alertar o bloquear compilaciones inseguras;

3.7. Capacidades de Integración

- Debe integrarse, como mínimo, con los siguientes orquestadores;
    - Kubernetes de vainilla;
    - Red Hat OpenShift;
    - Docker Swarm;
    - Motor Rancher Kubernetes
- Debe ser compatible y estar integrada a Jenkins Freestyle, Maven, Pipeline, CloudBees Core.
- Debe permitir la creación y aplicación de políticas granulares que proporcionen controles precisos sobre cada trabajo de CI (integración continua), como, por ejemplo, bloquear cualquier compilación afectada por una vulnerabilidad (CVE).

- La solución debe ser compatible con Open Policy Agent.
- Debe permitir crear reglas de admisión basado en el lenguaje REGO, el cual es propio de OPA.
- Debe poder aplicar políticas en microservicios, clústeres de Kubernetes, pipelines de CI / CD, API gateways.

3.8. Plataforma de Gestión y Monitoreo

- La solución debe ser implementada de forma local en una Nube Privada.
- Debe ser posible restringir el acceso a la interfaz de administración a direcciones o redes IP específicas o requerir MFA para el acceso a la consola;
- El acceso a la interfaz de administración debe realizarse a través de HTTPS con TLS 1.2 o superior;
- Debe ser posible crear usuarios locales o integrarse con la base de usuarios local, a través de SSO o federación
- Para las cuentas locales, debe ser posible configurar una política de contraseña, especificando su complejidad y período de rotación;
- Debe ser posible gestionar los permisos de los usuarios definiendo roles, con al menos roles de administrador, solo lectura y roles que limiten las funcionalidades a aprovisionamiento de plataformas de nube
- Debe contar con una herramienta de CLI que permitan realizar tareas de soporte sobre la plataforma de seguridad.
- Debe almacenar eventos de auditoria local sobre la plataforma, como mínimo debe registrar los accesos, runtimes (basado en procesos, red, archivos de sistema y llamadas de sistema), firewall y tareas administrativas. Estos eventos deben poder ser enviados a un servidor Syslog externo.

ANEXO A2

SOLUCIONES PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES

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

A. Levantamiento de Información

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

B. Instalación y configuración

1. 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.
2. Se debe crear como mínimo un usuario por cada rol existente en la plataforma.
3. Se debe realizar otras configuraciones que el implementador considere necesario para el correcto funcionamiento de la plataforma.
4. Todas las soluciones deben instalarse a fin de que operen acorde a las buenas prácticas recomendadas por el fabricante de la plataforma.
5. Se debe documentar todos los procedimientos realizados en la implementación.
6. En caso se requiera instalar algún componente en la Nube Privada del MEF, este deberá ser indicada en la oferta técnica como requerimientos de despliegue, indicando los recursos necesarios.
7. Para el componente de seguridad de contenedores, se deberá contar con personal especializado en seguridad de Containers y Kubernetes.

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:
    - 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

SOLUCIONES PARA LA PROTECCIÓN DE AMBIENTES VIRTUALES

CONTRATACIÓN DEL SERVICIO DE CONTINUIDAD OPERATIVA

1. Consideraciones generales

- Este servicio cubrirá todo el hardware y 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.
- La asistencia técnica necesaria será brindada por personal técnico calificado y especializado en los productos ofrecidos, quien deberá estar debidamente capacitado para dicha labor.
- 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.
- 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, por vía telefónica o por mensajería instantánea. 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 el registro o reportes de incidentes, fallas, problemas y requerimientos, según corresponda, así como también realizar el seguimiento, monitoreo de estado de los componentes de la solución, 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 trabajo, 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.
- Se deberá asignar a un especialista como “Personal Residente” en las instalaciones del Ministerio en el horario de oficina (de lunes a viernes de 9:00 a 18:00 horas) a fin de monitorear la solución ofertada y realizar las configuraciones que hubiese, por el periodo de mil noventa y cinco (1095) días calendario, que iniciaran una vez firmada la conformidad de la prestación principal. Previa coordinación con el personal de la OGTI del MEF se prestarán los servicios de manera remota.
- 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.
- 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 revisar y evaluar el estado de la solución materia del presente contrato. El contratista, de detectar un imperfecto o anomalía deberá realizar cualquier ajuste necesario para su corrección.
- 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. 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 ser brindada dentro de los primeros noventa (90) días calendario del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- 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 por cada uno de los componentes que forman parte del Item paquete 02. 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 (fuera del horario de oficina) y sábados.

2.3.1. 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.

2.3.2. 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, 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.

2.4. 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.

2.4.1. 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.

2.4.2. 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 del 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.

2.4.3. Servicio de Capacitación

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 capacitación, según detalle:

- Documento de Capacitación.
  - Nombre del personal
  - Temario
  - Cantidad de horas de la capacitación brindada.
  - Certificados de los participantes de la capacitación.

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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Incidencias Corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo en la solución	**Alto**	**Tiempo de respuesta:** 30 minutos **Tiempo de solución:** 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.
	Medio	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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.
	Bajo	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Requerimiento Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	**Medio**	**Tiempo de Respuesta** 2 horas **Tiempo de Solución** 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.

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 I o implementador II 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. 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.

Personal de capacitación: Será la persona encargada de brindar la capacitación en el manejo de la solución ofertada al personal designado por la OIT.
El personal para la capacitación debe estar avalado por la marca para brindar la capacitación oficial.

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	Incumplimiento De Programa O Ejecución De Trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	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 del servicio (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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
5	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:

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

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:

THM = 24 x 90 = 2,160 horas

THE = 4+3 = 7 horas

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

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%

Rango de UPTIME	Penalidad(1)
>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 calendario, 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 Tecnología 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, 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 Capacitación, se realizará un solo pago, luego de emitida la conformidad, previa presentación del Documento de Capacitación.
- Para el Servicio de Mantenimiento Preventivo, se realizará en seis (6) pagos en partes iguales, luego de emitida la conformidad previa presentación del informe por la realización del servicio.

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 perdida 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.

El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria 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 dictadas 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 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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.

ANEXO A4

Solución para la protección de ambientes virtuales

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.**
1. Solución para la Protección de Ambientes SDDC (Software Defined Data Center)				
El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS				
No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.				
Cada equipo NGFW debe soportar hasta 800 mil sesiones de conexiones simultaneas				
Deberá integrarse de forma nativa con la solución de VMware NSX Manager versión 6.4 o superior, sin necesidad de hacer uso de software o plataformas terceras.				

Debe permitir el redireccionamiento del tráfico entre los host o grupos de host de la plataforma virtual al NGFW de manera nativa y automática, para ello deberá estar integrado al hypervisor.				
Debe tener control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, usuarios y grupos de usuarios, aplicaciones grupos estáticos y dinámicos de aplicaciones.				
Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.				
Debe reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, bases de datos, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, storage, comportamiento de archivos, servicios de autenticación.				
Para tráfico cifrado (SSL/TLS y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;				
Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante.				
Cuando se utilicen las funciones de Prevención de Amenazas el equipamiento debe entregar el mismo performance (no degradar) entre tener una única firma de seguridad habilitada o tener todas las firmas habilitadas.				
Debe soportar granularidad en las políticas de IPS, Antivirus y AntisSpyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.				
Debe ser capaz de inspeccionar malware que se propague por los protocolos HTTP, HTTP/2, FTP, SMB, SMTP, tanto en IPv4 como en IPv6.				
Debe soportar la inspección de archivos transferidos por los protocolos HTTP, HTTP/2, FTP, SMB, SMTP, tanto en IPv4 como en IPv6				
La solución deberá contar con una consola de administración centralizada para la gestión y administración de todos los NGFW.				
2. Solución para la Protección de Contenedores y Gestor de Contenedores				

Deberá consistir en una plataforma de protección de la carga de trabajo en la nube (CWPP: Cloud Workload Protection) proporcionando seguridad y protección de las cargas de trabajo en entornos de nube privada.				
La solución debe proteger automáticamente los contenedores, imágenes, registros, cargas de trabajo, aprendiendo sus características y comportamientos y aplicar políticas de seguridad en tiempo de ejecución o runtime.				
La solución deberá proveer un CMDB (Base de datos de recursos y configuraciones) en consola gráfica y API				
Capacidad de monitoreo continuo en los entornos de nube privada para ayudar a garantizar que la infraestructura de nube esté protegida contra amenazas de seguridad.				
Deberá tener la capacidad de detección y respuesta de amenazas para configuraciones incorrectas de recursos y vulnerabilidades de los contenedores y proporcionar visibilidad de la actividad del usuario dentro de cada entorno de la nube privada.				
La solución debe monitorear continuamente los activos de nube y validar cumplimientos de normas de seguridad y estándares de cumplimiento de la industria				
La solución debe contener como mínimo los siguientes estándares de cumplimiento: CIS (Center for Internet Security) GDPR, HIPPA, NIST 800-190.				
Debería permitir la creación de nuevos estándares de cumplimiento personalizados, para reflejar los estándares de la organización.				
Los nuevos estándares de cumplimiento deben poder ser definidos en base a Contenedores, Imágenes, Hosts.				
Debe tener un panel de cumplimiento que muestre la postura de cumplimiento de los entornos de nube monitoreados con los diversos estándares existentes				
El escáner de imágenes debe buscas malware en binarios en las capas de imágenes, incluida la capa base.				
Debe contar con un Dashboard que permita identificar las vulnerabilidades identificadas en los Contenedores, Registros, Imágenes, repositorios de código.				

Debe categorizar la criticidad de cada vulnerabilidad identificada y otorgar una puntuación de riesgo, que permita al administrador priorizar las vulnerabilidades a atender.				
Debe mostrar al menos la siguiente información de cada vulnerabilidad identificada: nivel de criticidad, complejidad y vector de ataque, disponibilidad del parche e identificación CVE.				
Deberá mostrar el repositorio de código y la ruta del archivo que presenta la vulnerabilidad, así como el registro y la imagen.				
Cada política debe permitir la definición de un nivel de severidad, disponibilidad de un parche, excepciones basadas en CVE, cluster, contenedor, imagen, namespace, repositorio de código.				
Debe permitir la investigación de incidentes detectados mediante el análisis de la configuración de los recursos en la nube, consumiendo datos de configuración de las API de los servicios de las plataformas en la nube administradas.				
Debe permitir la investigación de incidentes detectados a través de registros de auditoría, consumiendo datos y eventos del usuario de los servicios de las plataformas de nube administradas, permitiendo la investigación de accesos de consola y API, el monitoreo de actividades privilegiadas y la detección compromisos de cuenta.				
Debe permitir la investigación de incidentes de red, consumir y monitorear el tráfico de red (flujos de tráfico) de servicios en la nube, permitiendo la consulta de eventos de red en plataformas de nube administradas. Debe detectar cuándo los servicios, aplicaciones o bases de datos están expuestos a Internet y si hay intentos potenciales de extraer datos				
Debe identificar cuándo las direcciones IP sospechosas acceden a los recursos monitoreados				
Debe ser posible configurar remediación automática para violaciones de políticas de seguridad				
Debe tener la capacidad de integración para enviar registros y alertas para herramientas SIEM e integración con herramientas de orquestación y automatización de respuesta a incidentes (SOAR)				
Debe admitir la integración con herramientas de tickets como ServiceNow, JIRA.				

Debe permitir enviar alertas por Correo, plataformas SOAR, Slack y ser personalizable con Webhook.				
Protección en runtime para sistemas operativos Linux, con control de aplicaciones, lista blanca y sistema de archivos;				
Debe integrarse, como mínimo, con los siguientes orquestadores: Kubernetes de vainilla; Red Hat OpenShift; Docker Swarm; Motor Rancher Kubernetes				
La solución no debe insertar componentes como bibliotecas o agentes en los contenedores o imágenes;				
La solución debe soportar automáticamente el crecimiento del clúster, sin requerir intervención manual en el proceso de protección de nuevos nodos;				
La solución debe gestionar y evitar vulnerabilidades desde el desarrollo hasta la producción, integrándose con el proceso de CI (integración continua) a través de plug-ins o mediante la interfaz de línea de comandos (CLI), en el registro y en producción para identificar y priorizar vulnerabilidades y riesgos en contenedores, imágenes y registros.				
Debe ser compatible y estar integrada a Jenkins Freestyle, Maven, Pipeline, CloudBees Core.				
La solución debe ser compatible con Open Policy Agent.				
Debe poder aplicar políticas en microservicios, clústeres de Kubernetes, pipelines de CI / CD, API gateways.				
Debe permitir crear reglas de admisión basado en el lenguaje REGO, el cual es propio de OPA.				
La solución debe ser implementada de forma local en una Nube Privada.				
Debe ser posible restringir el acceso a la interfaz de administración a direcciones o redes IP específicas o requerir MFA para el acceso a la consola;				
El acceso a la interfaz de administración debe realizarse a través de HTTPS con TLS 1.2 o superior;				
Debe ser posible crear usuarios locales o integrarse con la base de usuarios local, a través de SSO o federación				

ITEM PAQUETE 03

CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA TOMA DE EVIDENCIAS DIGITALES DE LA INFRAESTRUCTURA TECNOLÓGICA DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.

ESPECIFICACIONES TÉCNICAS
CONTRATACIÓN DE SOLUCIONES DE CIBERSEGURIDAD PARA LA TOMA DE EVIDENCIAS DIGITALES 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 toma de evidencias digitales 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 toma de evidencias digitales 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 evolución acelerada de los ataques cibernéticos requiere una implementación de nuevos componentes tecnológicos de protección que permitan hacer frente a las nuevas amenazas cibernéticas orientadas específicamente a los servicios tecnológicos que ofrece el MEF a sus distintos usuarios internos y externos.

5. Objetivo De La Contratación

5.1 Objetivo General

Implementar soluciones para la toma de evidencias digitales de la Infraestructura Tecnológica del MEF.

5.2 Objetivo Específico

- ✓ Establecer capacidades para la toma de evidencias digitales.

6. Alcance y descripción de los bienes a contratar

6.1 Descripción y cantidad de los bienes

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

ITEM PAQUETE 03

Solución para toma de evidencias digitales		
Prestación	**Descripción**	**Cantidad**
Principal	Software de extracción de datos de computadoras	1
	Equipo de extracción de datos de dispositivos	1

	Software de análisis de datos digitales extraídos	1
	Servidor de análisis de datos extraídos FRED	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

6.2 Distribución de la solución

En el siguiente cuadro muestra la distribución de los componentes de la solución teniendo en cuenta su ubicación:

Ítem Paquete 03

Software de extracción de datos de computadoras

- Deberá estar implementado en el centro de datos Principal.

Equipo de extracción de datos de dispositivos

- Deberá estar implementado en los centros de datos Principal, Contingencia.

Software de análisis de datos digitales extraídos

- Deberá estar implementado en el centro de datos Principal.

Servidor de análisis de datos extraídos FRED

- 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 una solución de ciberseguridad para la toma de evidencias digitales 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 El contratista deberá ofertar la última versión disponible del Hardware y/o Software del fabricante. 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.
- ✓ 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, para la cual 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 la 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 software requeridos en el **ANEXO A1,** los mismos que deben cumplir como mínimo con las siguientes características técnicas:

ITEM PAQUETE 03

Solución para toma de evidencias digitales	
Descripción	Anexo
Características Técnicas de la Solución de Seguridad para Desarrollo de Aplicaciones y Servicios Seguros	A1

7.2.2 Implementación: Levantamiento de información, instalación, configuración, pruebas y puesta en marcha.

El Contratista deberá implementar el equipamiento de hardware y/o software 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 todos los servidores y herramientas proporcionadas (Hardware y/o Software), todo el cableado y su etiquetado (energía, redes), los switch..
- ✓ Los requerimientos específicos del ítem paquete 03 se detallan en el anexo A2.

ITEM PAQUETE 03

Ítem Paquete 03	
Solución para toma de evidencias digitales	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	A2

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 emitida la Conformidad de la Prestación Principal. Esta garantía debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 del día siguiente de emitida la Conformidad de la Prestación Principal. Esto debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 equipamiento o hasta que se encuentren vigentes por el fabricante.
- ✓ La garantía de los equipos suministrados será por un período de mil noventa y cinco (1095) días calendario, contado a partir del día siguiente de emitida la Conformidad, 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.
- ✓ Todos los componentes de la Plataforma Tecnológica propuesta no podrán presentar adulteraciones ni correcciones (por ejemplo: tarjeta madre, fuente, etc.).

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 Accesoria a los bienes ofertados en la Prestación Principal (Anexo A1)

Los requerimientos específicos del ítem paquete 03 se detallan en el anexo A3.

ITEM PAQUETE 03

Ítem Paquete 03	
Solución para toma de evidencias digitales	
Descripción	Anexo
Servicio de continuidad operativa	A3

12. FUNCIONES DEL PERSONAL

Se detalla las funciones del personal:

ITEM PAQUETE 03

Ítem Paquete 03			
Solución para toma de evidencias digitales			
Cant.	Personal	Perfil	Actividades
1	Coordinador (Personal Clave)	• Titulado en Administración o Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería electrónica o Ingeniería de las telecomunicaciones o Ingeniería de Computación y Sistemas. • Certificación de PMP (Project Management Professional). • Experiencia mínima de tres (03) años en servicios de implementación o soporte en las soluciones de ciberseguridad ofertada y/o en alguno de sus componentes y/o en bienes que integran la solución ofertada, del personal clave requerido como Coordinador.	• Coordinar la implementación de la solución. • Coordinar con el encargado del área de la OGTI del MEF. • Coordinar con los implementadores de su empresa para el cumplimiento de los objetivos en el tiempo planificado. • Reportar a la OGTI los avances según el cronograma establecido en el plan de trabajo. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana).
1	Implementador I (Personal Clave)	• Ingeniero titulado 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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en la solución ofertada, Se	• Análisis de los detalles técnicos de la tecnología que se va implementar, ya sean especificaciones de hardware, de software, de licenciamiento. • Pruebas de laboratorio, que certifiquen el procedimiento de implementación y las funcionalidades técnicas del producto. • Instalación y configuración de la solución. • Pruebas de la solución implementada. • Elaboración de la documentación de la solución implementada. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). • Otros requerimientos asignados por el Jefe de Proyecto.

		aceptará certificado oficial de las marcas que conformen la solución. No se aceptará certificaciones de venta o pre venta. • Experiencia mínima de tres (03) años en servicios de implementación o soporte en las soluciones de ciberseguridad ofertada y/o en alguno de sus componentes y/o en bienes que integran la solución ofertada, del personal clave requerido como Implementador I.	
1	Implementador II	• 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. • Certificado Oficial de nivel profesional o ingeniería o administración o experto en la solución ofertada, Se aceptará certificado oficial de las marcas que conformen la solución. No se aceptará certificaciones de venta o pre venta.	• Levantamiento de información de la infraestructura del MEF. • Apoyo en la instalación y configuración de la solución ofertada. • Apoyo en la elaboración de la documentación de la solución implementada. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). • Otros requerimientos asignados por el Jefe de Proyecto.

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

ITEM PAQUETE 03

Ítem Paquete 03		
Solución para toma de evidencias digitales		
Prestación	**Descripción**	**Cantidad**
Principal	Software de extracción de datos de computadoras	1
	Equipo de extracción de datos de dispositivos	1
	Software de análisis de datos digitales extraídos	1
	Servidor de análisis de datos extraídos FRED	1
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	1
Accesoria	Servicio de continuidad operativa • Soporte Técnico • Mantenimiento Preventivo • Capacitación	1

Por motivo que los bienes y servicios se encuentran relacionados entre sí, se considera conveniente realizar contrataciones 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 disgregada 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 cada paquete.

15.1 Cumplimiento 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 de la prestación 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.

15.2 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 perdida 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.

15.3 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. El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria General N° 007-2014-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.

Las adecuación e 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° 972-2020-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 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° 972-2020-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 nitrito, 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 serologías o moleculares para COVID-19 es potestativo, salvo que el Ministerio identifique un caso sospechoso del personal propuesto, en tal sentido se autorizara el cambio del personal, luego del reporte del área usuaria de la Entidad.

17. Otros documentos

17.1 Para la presentación de oferta

- ✓ Los postores deberán presentar la siguiente documentación: Folletos, brochures, certificados, enlaces web, 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, 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.
- ✓ Documentación donde se indique de manera detallada el peso (kg), espacio (m2), disipación de energía (BTU/hr) y energía eléctrica (watts), de cada uno de los equipos ofertados según corresponda.
- ✓ 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 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° 972-2020-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

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 instalará la solución ofertada, 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

El plazo máximo de entrega de los bienes de la prestación principal, de los equipos que se detallan en el Anexo A1 es de cincuenta (50) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

Plazo de implementación

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

20. 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.

Para cada ítem paquete 03 se deberá 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, sitio en Jr. Lampa N° 274 - Cercado de Lima, 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.
- Actividades a realizar.
- 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.
- Hitos de implementación.
- Diagrama Gantt (Cronograma)
- Horarios de trabajo
- Configuraciones propuestas en la solución ofertada
- Procedimientos de inspección.
- Documentación del personal responsable para las coordinaciones administrativas para llevar el control sobre la prestación accesoria.
- Documentación del personal propuesto que brindará la asistencia técnica de la prestación accesoria y deberá contar como mínimo con el perfil y experiencia solicitada.
- Responsabilidades y consideraciones.
- Análisis y gestión de riesgos
  - Identificación de riesgos
  - Valoración de riesgos
  - Controles a implementar
  - Plan de vuelta atrás

- Carta del fabricante que indique lo solicitado en el numeral 2.3 del Anexo A3 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 cincuenta (50) 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, sitio en Jr. Lampa N° 274 - Cercado de Lima.

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 implementación de la prestación principal, se deberá entregar un Informe Final, a través de mesa de parles del Ministerio, sitio en Jr. Lampa N° 274 - Cercado de Lima, necesario para que se otorgue la conformidad de la Prestación Principal, 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 todas las soluciones ofertadas en un dispositivo.
- 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 ofertados.
- Informe de Verificación de Cumplimiento de todos los requerimientos técnicos de las presentes especificaciones técnicas
- Informe de Conclusiones y Recomendaciones

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.

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.

22. Adelantos

La entidad podrá otorgar un adelanto directo hasta por 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, adjuntando 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 aplicara las siguientes penalidades, de acuerdo con lo dispuesto por el artículo 161° y 163º 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	Incumplimiento de programa o ejecución de trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	Por incumplimiento de participación del personal Cuando se detecte que EL CONTRATISTA envía a un personal clave 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.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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.
5	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

ITEM PAQUETE 03

Ítem Paquete 03	
Anexo A1	Características técnicas de la Solución para toma de evidencias digitales
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

1. Experiencia del Postor en la Especialidad

Para el Ítem Paquete 03, se debe considerar lo siguiente:
Requisitos:
El postor debe acreditar un monto facturado acumulado equivalente a S/ 4´000,000.00 (Cuatro Millones con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran similares a los siguientes:

- Venta o Adquisición de solución de seguridad informática.
- Venta o Adquisición de equipamiento de seguridad perimetral.
- Venta o Adquisición de equipamiento de seguridad de TI.
- Venta o Adquisición de solución forense digital.
- Venta o Adquisición de servidor FRED.
- Venta o Adquisición de software forense digital.

Acreditación para el ítem paquete 03:
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.

2. Capacidad técnica y profesional

B.1. Experiencia de Personal Clave para el ítem paquete 03:

Requisitito
Coordinador
Experiencia mínima de tres (03) años en servicios de implementación o soporte en las soluciones de ciberseguridad ofertada y/o en alguno de sus componentes y/o en bienes que integran la solución ofertada, del personal clave requerido como **Coordinador**.

Implementador I
Experiencia mínima de tres (03) años en servicios de implementación o soporte en las soluciones de ciberseguridad ofertada y/o en alguno de sus componentes y/o en bienes que integran la solución ofertada, del personal clave requerido como **Implementador I**

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 TOMA DE EVIDENCIAS DIGITALES

A. Software de extracción de datos de computadoras

1. Debe contar con licenciamiento perpetuo con actualizaciones por mil noventa y cinco (1095) días calendario sin límite de extracción de dispositivos.
2. Debe contar con una interfaz fácil de usar que permite buscar, filtrar y depurar fácilmente grandes conjuntos de datos,
3. Debe realizar análisis inteligentes de datos sobre Windows Vista a Windows 10
4. Debe revisar el historial del dispositivo desde Microsoft Volume Shadow Copies
5. Debe realizar análisis de la memoria incorporada de Windows y de los registros de Windows
6. Debe analizar automáticamente como mínimo la información de la cuenta, documentos recientes, descargas, papelera de reciclaje, conexiones USB.

B. Equipo de extracción de datos de dispositivos

1. Debe contar con licenciamiento perpetuo con actualizaciones por mil noventa y cinco (1095) días calendario sin límite de extracción de dispositivos.
2. Tableta rugerizada con pantalla multitáctil capacitiva con resolución de 1024 pixeles, para facilidad de uso en condiciones de sol brillante o baja iluminación. Debe incluir:
   - Lector multi-SIM incorporado
   - Memoria DDR3
   - Wi-Fi b\g\n\ac - (hasta 350 Mbps)
   - Disco duro rápido y grande (SSD 128 GB)
   - Puerto DisplayPort
   - Sistema operativo incorporado compatible con la solución propuesta.
   - 4x puertos USB3.1 fase 1, 1,5 A por puerto, compatibilidad parcial con BC1.2
   - Puerto serial especial para teléfonos móviles de gama media
   - SIM, Micro SIM y Nano SIM
   - Mini DisplayPort 1.3
   - 10/100/1000 Ethernet
   - Altavoces estéreo de 0,5 W | Micrófono | Zumbador
   - Incluye maletín de protección, múltiples conectores y cables USB (30 unidades mínimo) para distintos modelos de celulares, fuente de poder para la tableta, 10 bolsa Faraday
3. La herramienta debe permitir la función de detección automática: detecta automáticamente el perfil del dispositivo para la extracción cuando se conecta a una amplia variedad de dispositivos.
4. Perfiles dinámicos: la función aprovecha una base de datos única que recomienda automáticamente métodos de extracción alternativos para dispositivos no probados en función de la información del dispositivo.
5. Perfiles de extracción genéricos para seleccionar en función de la versión del sistema operativo y el conjunto de chips.
6. Perfiles de extracción: Debe admitir más de 28,000 perfiles de dispositivos para la extracción.

7. Extracción de copia rápida: debe permitir explorar el sistema de archivos del dispositivo de destino y extraer selectivamente datos multimedia.
8. Debe permitir extracción lógica y física sin pasar por el bloqueo de usuario para numerosos dispositivos, incluidos los siguientes fabricantes:
9. Akai, AU, AceMobile, Acer, Alcatel, Allview, Amoi, Archos, Ark, Asus, Audiovox, BLU, BQ, Beafon, Blackview, Bluboo, Bmobile, CAT, Cal Comp, Cherry Mobile, Coolpad, Cubot, Daxian, Digicel, Donod, Doogee, Doro, Elephone, Explay, Fly, G-Tide, GOMobile, GeeksPhone, GeneralMobile, Gionee, HTC, Orange (SPV), T-Mobile, Haier, Hisense, Homtom, Huawei, I-Mobile, IUNI, IUSACELL, Infinix, Intex, Jaga, Jugate, Just5, K-Touch, Karbonn, Kazam, Kyocera, LYF, Lanix, Lava, LeTV, Lenevo, LG, M4Tel, MLS, MTC, Marshall, Maxwest, Meizu, Micromax, MobiWire, Mobistel, Atelier HC, Motorola, MyPhone, NTT Docomo, NYX, NiU, Nokia, NuuMobile, OnePlus, Oppo, Oysters, POSH, MIO, PanTech, Philips, Polaroid, Prestigio, QMobile, RCA, RugGear, SFR, Sagem, Samsung, Sanyo, Sky, Softbank,
10. El sistema debe permitir recuperar archivos borrados.
11. Debe permitir reconstruir páginas web, a partir de archivos de caché. Con esta capacidad, podrá ver el contenido del sitio web sin conexión con el contenido del caché del navegador.
12. Debe permitir la detección de malware para iOS, Android, BlackBerry
13. Debe de contar con asistente SQLITE
14. Debe de contar con un Analizador virtual : un emulador que pueda mostrar evidencia digital forense de más de 3 millones de aplicaciones de Android.
15. Debe proporcionar acceso a la traducción para más de 40 idiomas, disponibles en 120 convenientes pares de idiomas.

Capacidades de extracción sobre Android

16. Extracción lógica: Contacts, SMS, MMS, Calendar, Pictures, Audio, registro de llamadas, mensajeria instantánea, etc
17. Extracción parcial del sistema de archivos sin pasar por el bloqueo de usuario: Soporte para más de 600 dispositivos. Para dispositivos con SO hasta 5.1.1 inclusive, se pueden extraer SMS, MMS, cuentas de usuario, contraseñas, aplicaciones instaladas, diccionarios de usuarios, imágenes / videos y archivos de datos. Para dispositivos que ejecutan OS 6.x, se debe extraer archivos imágenes y videos.
18. Extracción selectiva del sistema de archivos completo de dispositivos Android: debe extraer datos desde el sistema de archivos completo, como mensajes de WhatsApp, mensajes de Facebook, correos electrónicos.
19. Extracción selectiva de tokens en la nube de dispositivos Android: debe permitir extracción tokens de nube a los que solo se puede acceder a través del sistema de archivos completo desde dispositivos bloqueados y encriptados.
20. Capacidad genérica de Android LockPick: el sistema debe permitir omitir la pantalla de bloqueo en fabricantes de dispositivos como Samsung, LG, Motorola, Sony, Xiaomi con Android OS 6.0 y superior.
21. Desactivación de contraseña de Android con capacidades de reactivación para Acer, Alcatel, Allview, BLU, Blackview, CAT, Coolpad, Cubot, Doogee, Doro, Elephone, Gionee, HTC, Homtom, Huawei, Infinix, LeTV, Lenovo, LG, MLS, Meizu , Micromax, Motorola, NTT Docomo, Nokia, Qmobile, Samsung, Tecno, Ulefone, VIVO, Vodafone, Wiko, ZTE.

22. Extracción física avanzada de ADB: capacidad de realizar extracciones físicas donde para dispositivos Android con versiones del sistema operativo hasta 7.1 con nivel de parche de seguridad hasta noviembre de 2016.
23. El sistema debe omitir el bloqueo de usuario y realizar la extracción física descifrada de dispositivos bloqueados y cifrados con el chipset Qualcomm. Debe admitir chips genéricos 8909, 8916, 8936, 8939 y 8952 , además chips compatibles 8917, 8937, 8940 y 8953.
24. Entre los dispositivos probados se encuentra el soporte para dispositivos fabricados por Asus, Samsung, ZTE, Xiaomi, VIVO, Huawei, Motorola, Kyocera, Orange (SPV), CAT, Alcatel, Vertu. Además, miles de dispositivos adicionales que poseen conjuntos de chips Qualcomm son genéricamente compatibles, incluso dispositivos que no son Android, como los dispositivos KaiOS como ejemplo.
25. Debe proporciona una técnica no invasiva para evitar bloqueos, superar el cifrado y realizar extracciones físicas y completas del sistema de archivos en los modelos de dispositivos Samsung que usan conjuntos de chips Qualcomm 8917, 8937, 8940, 8952, 8953, 8976, 8996 y SDM450.
26. El sistema debe permitir la extracción física de más de 80 modelos de chipset MTK.
27. Extracción física para Huawei, Motorola, Wiko y otros dispositivos Android que incluyen: Huawei Y560-L01, Huawei Watch 2608, Motorola XT1526 Moto E 2nd Gen y más.

Capacidades de extracción sobre iOS.

28. Debe permitir la extracción lógica de contactos, SMS, MMS, calendario, imágenes, audio, video, registros de llamadas, correo electrónico, mensajería instantánea y datos de navegación desde dispositivos iOS.
29. Debe permitir extracción lógica avanzada: debe utilizar otros protocolos de extracción y extraer datos adicionales en comparación con la extracción lógica estándar. Con opción para cifrar el archivo de copia de seguridad de iTunes.
30. Debe permitir realizar rápidamente un jailbreak temporal forense y una extracción completa del sistema de archivos dentro de un flujo de trabajo optimizado para dispositivos Apple desde iPhone 4s hasta la última versión de iPhone 10.
31. Debe permitir extracciones de BFU con alto rendimiento de extracción de datos que incluyen notificaciones, correo electrónico, correo de voz, imágenes, videos, documentos de notas de voz, cookies, bases de datos, redes inalámbricas, cuentas de usuario, ID de Apple y más.
32. Capacidad para extraer datos de muchas fuentes de datos:
    Amazon Alexa, Amazon Shopping, Booking, Box, Coinbase, DJI Go 4, Dropbox, Facebook, Facebook Messenger, FitBit, Generic Email (IMAP), Gmail, Google Backup, Google Calendar, Google Chrome Sync, Google Contacts, Google Drive, Google Hangouts, Google Home, Google Keep, Google Location History, Google My Activity, Google Passwords, Google Photos, Google Takeout, Google Tasks, Google Recent Devices, Google Backup, iCloud (Real Time Locations), iCloud Backup (2FA is supported for iOS 12.4.x), iCloud Applications, iCloud Calendars, iCloud Call History, iCloud Contacts, iCloud iTunes, iCloud Drive, iCloud Notes, iCloud Photos, iCloud Safari Bookmarks, iCloud Safari History, Microsoft Office 365, Instagram, LinkedIn, Lyft, Magenta Cloud, Samsung Backup, Skypixel,

OkCupid, Microsoft Outlook 365, One Drive, Password Collector, Uber, Skype, Slack, Telegram, Twitter, Viber Backup (Google Drive),Viber Backup (iCloud), WhatsApp Backup (Google Drive), WhatsApp Backup (iCloud), and VKontakte.

C. Software de análisis de datos digitales extraídos

1. Debe contar con licenciamiento perpetuo con actualizaciones por mil noventa y cinco (1095) días calendario para un mínimo de 5 operadores y 500 extracciones.
2. Debe contar con módulo de análisis de vínculos que debe permitir el análisis de informaciones de hasta de 1500 fuentes digitales de datos.
3. La herramienta debe permitir subir archivos, en al menos en los siguientes formatos:o ZIP, o RAR, o DD, o RAW, o E01, o XML, o IMG, o BIN, o FAT /FAT16 / FAT32, o exFATo NTFS, o Apple HTF/HFS+ ,o EXT2/EXT3/EXT4.
4. La herramienta debe permitir subir y procesar información de 500 extracciones:
    - Imágenes espejo y/o datos de computadores.
    - Imágenes espejo y/o videos de dispositivos DVR.
    - Documentos digitales de software y/o aplicaciones de ofimática.
    - Documentos físicos escaneados para ser procesados por OCR.
5. La herramienta debe permitir investigar los vínculos, datos en común, relaciones, intercambio de información, ubicaciones en común y asociaciones entre los dispositivos y sus usuarios adicionalmente.
6. Debe poder clasificar las imágenes y videos presentes en las diferentes extracciones.
7. Debe posibilitar a partir de más de una extracción correlacionar las informaciones comunes entre los usuarios, incluyendo:
    - SMS.
    - MMS.
    - Llamadas telefónicas.
    - Chats.
    - Conversaciones de Mensajería Instantánea.
    - Correos Electrónicos.
    - Ubicaciones Geográficas.
    - Agenda de Contactos.
8. Debe permitir la generación de informes a partir de las informaciones generadas en al menos los siguientes formatos:
    - PDF.
    - XLS.
    - DOC.
9. Debe permitir la visualización de la correlación entre la información en formato gráfico, como una red de contactos entrelazada cuando aplicare el caso, siendo posible cambiar la ubicación en la interfaz gráfica de los objetos analizados conforme la necesidad.
10. Debe poder cambiar la vista grafica al menos según:
    - Contactos con conexionas entre varios dueños de una fuente de datos digital.
    - Número mínimo de interacciones.
    - El sentido de las Interacciones.
    - El volumen de las interacciones

11. La herramienta debe permitir la visualización de la correlación entre la información en también en formato tabular, como una tabla de eventos en orden cronológico.
12. La herramienta debe tener un panel donde puedan verse los contactos con los que un dueño de dispositivo tuvo más interacciones.
13. Debe tener un panel donde pueda verse si un dueño de dispositivo tiene coincidencias en su dispositivo contra una lista de palabras claves de la que se ejecutó una búsqueda.
14. Debe permitir la visualización de la información de las diversas extracciones e información en común entre ellas en orden cronológico en el formato de línea de tiempo “timeline”, a fin de investigar la secuencia lógica y cronológica de los hechos comunes.
15. La herramienta debe permitir la visualización en mapa de todos los hechos, eventos, datos y actividades, individuales y/o comunes que tengan información de la geolocalización generados por los individuos a quienes correspondan las extracciones.
16. Debe soportar correlación de dispositivos móviles como: teléfonos celulares, smartphones, tarjetas de memoria, dispositivos GPS y etc. Adicionalmente soportar archivos provenientes de la herramienta de extracción de datos en la nube.
17. Debe permitir el análisis y correlación de archivos de fuentes de datos digitales móviles con múltiples extracciones.
18. La herramienta debe estar disponible en por lo menos 12 idiomas, incluyendo inglés, portugués y español y debe permitir seleccionar hasta 5 idiomas de forma nativa para análisis de texto y OCR.
19. La herramienta debe permitir y soportar la importación de una lista de palabras claves para ejecutar la búsqueda de estas palabras en los dispositivos de un caso.
20. La herramienta debe permitir capturas de pantalla instantáneas
21. La herramienta debe permitir la aplicación de filtros a las informaciones analizadas, para reducir el volumen de eventos en al menos las siguientes categorías:
    - Período de tempo
    - Caso
    - Aplicaciones
    - SMS
    - Tipo de Evento
    - Fuente de Datos
    - Número mínimo de ocurrencias y actividades
    - Ocurrencias por fecha y hora
    - Palabras claves
22. Debe permitir el suministro de la palabra clave en campos de búsqueda entre toda la información disponible.
23. La herramienta debe permitir la personalización y emisión de informes.
24. Debe soportar datos de geolocalización a partir de fuentes, tales como: Torres de Telefonía Celular, Redes WiFi, GPSs, Aplicaciones que contengan datos o navegación.
25. Debe permitir el ingreso de 05 usuarios autorizados a través de un navegador web.
26. Debe permitir la creación de usuarios y contar con un sistema de usuario y contraseña para permitir o rechazar el ingreso a la misma.

27. Integrarse con un directorio activo para la gestión de usuarios.
28. La herramienta debe ser instalada en un servidor del contratante y se debe acceder por medio de un navegador web.
29. Debe tener la capacidad de identificar rostros y ejecutar búsquedas de rostros similares dentro de las imágenes existentes en las fuentes de información.
30. Debe tener la capacidad de hacer búsquedas de imágenes similares entre sí.
31. Debe identificar y transcribir palabras dentro de las imágenes por medio de OCR.
32. Debe permitir la identificación y clasificación automática de imágenes y videos en varias categorías predefinidas:
    - Armas.
    - Drogas.
    - Tatuajes.
    - Automóviles.
    - Capturas de Pantalla.
    - Documentos.
    - Rostros.
    - Desnudez.
    - Abuso Infantil o Abuso de menores.
33. Debe permitir al usuario administrador modificar los umbrales con los que hace la identificación y la categorización de imágenes y videos.
34. Debe permitir la creación de categorías propias, según las necesidades del usuario.
35. Debe también identificar de forma automática las imágenes y videos con contenido de una categoría propia.
36. Debe poder identificar automáticamente a un dueño de una fuente de datos digital según los identificadores presentes en la extracción, como email, IMEI, número de teléfono, etc.
37. Debe permitir exportar la totalidad de contactos y dueños identificados de las fuentes de datos digitales.
38. Debe permitir asignar un nombre provisto por el usuario a los contactos y dueños de dispositivos identificados y encontrados por la herramienta.
39. Debe permitir fusionar dos contactos y/o dueños de fuentes de datos que resulten ser la misma persona.

D. Servidor de análisis de datos extraídos FRED

Características del Servidor

1. Debe contar con licenciamiento perpetuo del sistema operativo con actualizaciones ilimitadas.
2. Fuente de alimentación redundante: 1600 Watt Modular cada una.
3. Chipset: deberá contar como minimó con 14 puertos USB, 14 puertos SATA, red de área local integrada.
4. Processor tipo dual 16-cores/32 Threads, 2.2 GHz/3.2 GHz
5. Turbo Speed, 22 MB Cache with liquid cooling
6. Lan adicional: Dual 10GB Ethernet (RJ45)
7. Video: de 24GB
8. Sound: 8 Canales (7.1) Codec de audio de alta definición con optical S/PDIF
9. OS Drive: 512GB M.2 NVMe SSD para Sistema Operativo.
10. Temp Drive: 2TB M.2 NVMe SSD para archivos temporales
11. Data Drive:4 X 4TB SAS Drives in RAID 5,6, or 10
12. Ventiladores Whisper Quiet de alta calidad en toda la unidad

13. 1 x 2.5" Bahía de intercambio en caliente con 4 bandejas extraibles para 2.5" SSD/HDD
14. RAM: 384GB
15. Sistema operativo incorporado compatible con la solución propuesta.
16. Bloqueador de escritura Tableau
17. Bahia para extracción de data de dispositivos móviles
18. 16X BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive
19. Teclado estándar 104 y mouse óptico.
20. Integrated LAN Dual Gigabit LAN Controller
21. Lector de tarjetas forense – Solo lectura (SD and MicroSD Cards)

ANEXO A2

SOLUCIÓN PARA TOMA DE EVIDENCIAS DIGITALES

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

A. Levantamiento de Información

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

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 crear como mínimo un usuario por cada rol existente en la plataforma.
4. Se debe realizar otras configuraciones que el implementador considere necesario para el correcto funcionamiento de la plataforma.
5. Todas las soluciones deben instalarse a fin de que operen acorde a las buenas prácticas recomendadas por el fabricante de la plataforma.
6. 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:
    a. 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.
    b. Detalle de las actividades a ejecutar y quién será el encargado de realizarlas, si la ENTIDAD o el CONTRATISTA.
    c. 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

SOLUCIÓN PARA TOMA DE EVIDENCIAS DIGITALES

CONTRATACIÓN DEL SERVICIO DE CONTINUIDAD OPERATIVA

1. Consideraciones generales

- Este servicio cubrirá todo el hardware y 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.
- La asistencia técnica necesaria será brindada por personal técnico calificado y especializado en los productos ofrecidos, quien deberá estar debidamente capacitado para dicha labor.
- Las labores técnicas a realizar sobre la solución se llevarán a cabo en el lugar donde éstos se encuentren instalados
- 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.
- 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, por vía telefónica o por mensajería instantánea. 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 el registro o reportes de incidentes, fallas, problemas y requerimientos, según corresponda, así como también realizar el seguimiento, monitoreo de estado de los componentes de la solución, 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 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 trabajo, 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, una vez al año, previa presentación del Plan de Trabajo por correo electrónico, según la siguiente tabla:

Mantenimiento	1	2	3
Mes	11	23	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.
- 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 revisar y evaluar el estado de la solución materia del presente contrato. El contratista, de detectar un imperfecto o anomalía deberá realizar cualquier ajuste necesario para su corrección.
- 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. 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 ser brindada dentro de los primeros noventa (90) días calendario del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- 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 uno de las personas debe recibir una capacitación mínima de cuarenta (40) horas por cada una de las cuatro (4) soluciones que componen el ítem paquete 03. 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 (fuera del horario de oficina) y sábados.

2.3.1. 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.

2.3.2. 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, 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.

2.4. 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.

2.4.1. 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 y presentación de los entregables mensuales.

2.4.2. 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 del 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.

2.4.3. Servicio de Capacitación

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 capacitación, según detalle:

- Documento de Capacitación.
    - Nombre del personal
    - Temario
    - Cantidad de horas de la capacitación brindada.
    - Certificados de los participantes de la capacitación.

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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Incidencias Corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo en la solución	**Alto**	**Tiempo de respuesta:** 30 minutos **Tiempo de solución:** 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.
	Medio	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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.
	Bajo	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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)

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Requerimiento Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	**Medio**	**Tiempo de Respuesta** 2 horas **Tiempo de Solución** 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.

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 I o implementador II 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. 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.

Personal de capacitación: Será la persona encargada de brindar la capacitación en el manejo de la solución ofertada al personal designado por la OIT.
El personal para la capacitación debe estar avalado por la marca para brindar la capacitación oficial.

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	Incumplimiento De Programa O Ejecución De Trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	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 del servicio (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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
5	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:

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

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:

THM = 24 x 90 = 2,160 horas

THE = 4+3 = 7 horas

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

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%

Rango de UPTIME	Penalidad(1)
>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 calendario, 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 Tecnología 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 Capacitación, se realizará un solo pago, luego de emitida la conformidad, previa presentación del Documento de Capacitación.
- Para el servicio de Mantenimiento preventivo, el pago se realizará en tres (3) 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.

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 perdida 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.
El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria 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 dictadas 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° 972-2020-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° 972-2020-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 nitrito, 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 serologías 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.

ANEXO A4

Solución para toma de evidencias digitales

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.**
1. Solución para toma de evidencias digitales					
A. Software de extracción de datos de computadoras					
1. Debe contar con una interfaz fácil de usar que permite buscar, filtrar y depurar fácilmente grandes conjuntos de datos,					
2. Debe realizar análisis inteligentes de datos sobre Windows Vista a Windows 10					
3. Debe analizar automáticamente como mínimo la información de la cuenta, documentos recientes, descargas, papelera de reciclaje, conexiones USB.					
B. Equipo de extracción de datos de dispositivos					
1. La herramienta debe permitir la función de detección automática: detecta automáticamente el perfil del dispositivo para la extracción cuando se conecta a una amplia variedad de dispositivos.					
2. Perfiles de extracción: Debe admitir más de 28,000 perfiles de dispositivos para la extracción.					
3. Extracción de copia rápida: debe permitir explorar el sistema de archivos del dispositivo de destino y extraer selectivamente datos multimedia.					
4. El sistema debe permitir recuperar archivos borrados.					
5. Debe de contar con un Analizador virtual: un emulador que pueda mostrar evidencia digital forense de más de 3 millones de aplicaciones de Android.					

Capacidades de extracción sobre Android				
6. Extracción selectiva del sistema de archivos completo de dispositivos Android: debe extraer datos desde el sistema de archivos completo, como mensajes de WhatsApp, mensajes de Facebook, correos electrónicos.				
7. Extracción selectiva de tokens en la nube de dispositivos Android: debe permitir extracción tokens de nube a los que solo se puede acceder a través del sistema de archivos completo desde dispositivos bloqueados y encriptados.				
8. El sistema debe permitir la extracción física de más de 80 modelos de chipset MTK.				
9. Extracción física para Huawei, Motorola, Wiko y otros dispositivos Android que incluyen: Huawei Y560-L01, Huawei Watch 2608, Motorola XT1526 Moto E 2nd Gen y más.				
Capacidades de extracción sobre iOS.				
10. Debe permitir la extracción lógica de contactos, SMS, MMS, calendario, imágenes, audio, video, registros de llamadas, correo electrónico, mensajería instantánea y datos de navegación desde dispositivos iOS.				
11. Debe permitir extracción lógica avanzada: debe utilizar otros protocolos de extracción y extraer datos adicionales en comparación con la extracción lógica estándar. Con opción para cifrar el archivo de copia de seguridad de iTunes.				
C. Software de análisis de datos digitales extraídos				
1. Debe contar con módulo de análisis de vínculos que debe permitir el análisis de informaciones de hasta de 1500 fuentes digitales de datos.				
2. Debe permitir la creación de usuarios y contar con un sistema de usuario y contraseña para permitir o rechazar el ingreso a la misma.				
3. Integrarse con un directorio activo para la gestión de usuarios.				
4. Debe tener la capacidad de identificar rostros y ejecutar búsquedas de rostros similares dentro de las imágenes existentes en las fuentes de información.				
5. Debe identificar y transcribir palabras dentro de las imágenes por medio de OCR.				
6. Debe permitir la creación de categorías propias, según las necesidades del usuario.				
7. Debe permitir exportar la totalidad de contactos y dueños identificados de las fuentes de datos digitales.				
D. Servidor de análisis de datos extraídos FRED				

Características del Servidor					
1. Fuente de alimentación redundante: 1600 Watt Modular cada una.					
2. Chipset: deberá contar como mínimo con 14 puertos USB, 14 puertos SATA, red de área local integrada.					
3. Processor tipo dual 16-cores/32 Threads, 2.2 GHz/3.2 GHz					
4. Turbo Speed, 22 MB Cache with liquid cooling					
5. Lan adicional: Dual 10GB Ethernet (RJ45)					
6. Video: de 24GB					
7. Sound: 8 Canales (7.1) Codec de audio de alta definición con optical S/PDIF					
8. OS Drive: 512GB M.2 NVMe SSD para Sistema Operativo.					
9. Temp Drive: 2TB M.2 NVMe SSD para archivos temporales					
10. Data Drive:4 X 4TB SAS Drives in RAID 5,6, or 10					
11. Ventiladores Whisper Quiet de alta calidad en toda la unidad					
12. 1 x 2.5" Bahía de intercambio en caliente con 4 bandejas extraíbles para 2.5" SSD/HDD					
13. RAM: 384GB					
14. Bloqueador de escritura Tableau					
15. Bahía para extracción de data de dispositivos móviles					
16. 16X BD-R/BD-RE/DVD±RW/CD±RW Blu-ray Burner Dual-Layer Combo Drive					
17. Integrated LAN Dual Gigabit LAN Controller					
18. Lector de tarjetas forense – Solo lectura (SD and MicroSD Cards)					

ITEM PAQUETE 04

CONTRATACIÓN DEL EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE TI DEL MINISTERIO DE ECONOMÍA Y FINANZAS, EN EL MARCO DE LA INVERSIÓN CON CÓDIGO ÚNICO 2455051.

ESPECIFICACIONES TÉCNICAS
CONTRATACIÓN DEL EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE TI 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 del Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI 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 el Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el 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 evolución acelerada de los ataques cibernéticos requiere una implementación de nuevos componentes tecnológicos de protección que permitan hacer frente a las nuevas amenazas cibernéticas. La complejidad de esos incidentes requiere implementar el Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI, donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el Ministerio de Economía y Finanzas.

5. Objetivo De La Contratación

5.1. Objetivo General

Implementar el equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI, donde se puedan realizar las actividades de coordinación, identificación, protección, detección, respuesta y recuperación frente a los ciberataques hacía los servicios tecnológicos que ofrece el Ministerio de Economía y Finanzas.

5.2. Objetivo Específico

- ✓ Centralizar la detección y anticipación de amenazas cibernéticas
- ✓ Centralizar las actividades de coordinación y respuesta de las amenazas cibernéticas.

6. Alcance y descripción de los bienes a contratar

6.1. Descripción y cantidad de los bienes

La presente adquisición está compuesta por bienes a contratar, los mismos que se describen en el siguiente cuadro:

ITEM PAQUETE 04

Equipamiento para el Centro de Ciberseguridad y Centro de Operaciones de TI del MEF		
Prestación	**Descripción**	**Cantidad**
Principal	Piso Técnico.	2
	Sistema de Iluminación.	2
	Control de Acceso.	2
	Construcción en seco, sellado, pintura de paredes, pisos y puertas.	2
	Falso Cielo Raso	1
	Sistema de Aire Acondicionado.	1
	Gabinete de Comunicaciones.	5
	Unidad de Distribución Energética (PDUs).	12
	Conmutador de Trasferencia Automático	14
	Sistema de Video Wall (3x2).	1
	Sistema de Video Wall (4x2)	1
	Controlador de Video Wall.	2
	Workstation.	19
	Plataforma de Gestión.	1
	Mobiliarios.	19
	Sistema Eléctrico Estabilizado y Comercial.	2
	Cableado Estructurado.	2
	Detección de Incendios.	2
	Cámaras IP	5
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha.	2
Accesoria	Servicio de continuidad operativa y transferencia de conocimiento • Soporte Técnico • Mantenimiento Preventivo • Capacitación	2

6.2. Distribución de las Soluciones

Todo lo solicitado en el Ítem paquete 04 será instalado en el Centro de Ciberseguridad del Quinto piso del edificio Principal y en el Centro de Operaciones de TI del segundo piso de la Casa Grace, distribuidos de la siguiente manera:

Equipamiento para el Centro de Ciberseguridad y Centro de Operaciones de TI del MEF				
Prestación	**Descripción**	**Cantidad**	**Centro de operaciones de TI**	**Centro de Ciberseguridad**
Principal	Piso Técnico.	2	1	1

	Sistema de Iluminación.	2	1	1
	Control de Acceso.	2	1	1
	Construcción en seco, sellado, pintura de paredes, pisos y puertas.	2	1	1
	Falso Cielo Raso	1	0	1
	Sistema de Aire Acondicionado.	1	0	1
	Gabinete de Comunicaciones.	5	0	5
	Unidad de Distribución Energética (PDUs).	12	0	12
	Conmutador de Trasferencia Automático	14	0	14
	Sistema de Video Wall (3x2).	1	0	1
	Sistema de Video Wall (4x2)	1	1	0
	Controlador de Video Wall.	2	1	1
	Workstation.	19	10	9
	Plataforma de Gestión.	1	0	1
	Mobiliarios.	19	10	9
	Sistema Eléctrico Estabilizado y Comercial.	2	1	1
	Cableado Estructurado.	2	1	1
	Detección de Incendios.	2	1	1
	Cámaras IP	5	0	5
	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha.	2	1	1
Accesoria	Servicio de continuidad operativa y transferencia de conocimiento • Soporte Técnico • Mantenimiento Preventivo • Capacitación	2	1	1

7. Características de los bienes y condiciones

7.1. Generalidades

Centro de Ciberseguridad del MEF

- ✓ El contratista deberá realizar el Equipamiento para el Centro de Ciberseguridad el cual deberá ser supervisado y aprobado por la Oficina de Infraestructura Tecnológica de la OGTI del MEF.
- ✓ Dentro del equipamiento del Centro de Ciberseguridad, está la actividad de realizar el diseño e implementación del Sistema Eléctrico Estabilizado y Comercial.
- ✓ Para el diseño e implementación del Sistema Eléctrico Estabilizado y Comercial, el contratista deberá considerar el equipamiento que se encuentra dentro de los gabinetes y el equipamiento nuevo a implementar, además deberá considerar entre los cálculos un 25%, para futuro crecimiento.

La potencia del equipamiento en los gabinetes es:

- Gabinete 7: 9,000 watts.
- Gabinete 8: 2,500 watts.
- Gabinete 9: 6,000 watts.
- Gabinete 10: 2,000 watts.
- Gabinete 12: 6,500 watts.
- Gabinete 5: 15,500 watts.
- Gabinete 4: 12,000 watts.

- ✓ El contratista deberá considerar en su propuesta el retiro del sistema eléctrico estabilizado actual (04 tomacorrientes estabilizados, cableado eléctrico estabilizado de los gabinetes existentes, 02 tableros de distribución de energía estabilizada (UPS)) y sistema eléctrico comercial (01 tablero de distribución comercial, ubicados en el Cuarto de Tableros, 01 interruptor, 04 luminarias adosadas, 07 luminarias empotradas instalación en falso techo). Los cableados eléctricos a retirar se encuentran en las áreas a intervenir: Centro de ciberseguridad, operadores, cuarto de tableros.
- ✓ Se deberá retirar las acometidas eléctricas de los 02 tableros de distribución de energía estabilizada (UPS), 01 tablero de distribución comercial. Todos los elementos retirados, serán entregados al MEF.
- ✓ El contratista deberá realizar la instalación, configuración, pruebas, actualización y puesta en marcha de toda la infraestructura (Hardware y 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. El proveedor deberá realizar la actividad de reubicar el equipamiento que se encuentran en los 08 gabinetes actuales a los nuevos gabinetes. Del apagado y encendido de los equipos, estará a cargo el personal del MEF. Cualquier configuración en los equipos de propiedad del MEF o terceros, estará a cargo del personal del MEF y/o soporte de los equipos.
- ✓ El contratista deberá instalar 05 gabinetes, y contemplar la reubicación de un gabinete existente (gabinete 7) en el área asignada (centro de gabinetes). La reubicación del gabinete, se realizará dentro del área a intervenir (3 metros aprox.).
- ✓ El contratista deberá considerar 14 Conmutadores de Transferencia Automáticos (ATS / STS).
- ✓ El contratista deberá suministrar 70 cables de poder de C13 – C14 de 14 AWG como mínimo de 2 metros de longitud, los mismos que será utilizados en la reubicación del equipamiento existente.
- ✓ La implementación deberá contemplar, la adecuación del ambiente, retiro del piso técnico existente, zonas A largo: (7.58mts x ancho: 3.00mts), zona B (largo: 7.58mts x ancho: 3.11mts) y zona C (largo: 4.36mts x ancho: 1.98mts) lamina 01, instalación de un nuevo piso técnico, (zonas A, B, C y D) lamina 01, Sistema de Control de Acceso, Cámaras IP, Video Wall, Sistema de Gestión, Sistema de Detección de Incendios, Aire Acondicionado, Sistema Eléctrico, Sistema de Cableado Estructurado y Mobiliarios. Para esto deberá tomar en cuenta lo solicitado en las características técnicas mínimas del anexo A1.
- ✓ Todo el equipamiento debe ser nuevo, sin uso y de reciente fabricación. No se aceptarán equipos usados o re manufacturados.
- ✓ El servicio que realizará la Contratista será llave en mano, incluirá el uso de sus propios recursos humanos, herramientas, útiles, materiales, equipos certificadores, fletes y seguros, por lo que el servicio deberá ser presupuestado a todo costo y por lo tanto al MEF no le debe significar costo adicional al propuesto por el Contratista.

- ✓ El servicio solicitado incluye el retiro del cableado existente, luminarias (04 luminarias adosadas y 07 luminarias empotradas en el techo falso), aire acondicionado existentes (02 equipos Split decorativo), techo falso con baldosas de yeso (30 mts2, la altura entre el techo y el falso techo es de 0.42 mts, entre el techo y el techo falso hay instalado tubería metálica del tipo EMT, con cables eléctricos para el sistema de luminarias), pared de drywall con alma de plancha metálica (6.80 mts lineal), suministro de materiales, la instalación de canalizaciones, tendido de cableado, conectorización, pruebas de certificación, obras civiles (refuerzo de pared de drywall para la instalación de los monitores del Video Wall, y tableros eléctricos), resane, pintado, retiro de desmonte, rotulación de cables y todo lo necesario para que la implementación quede operativo y apto para ser usado. El contratista deberá mover los cables de fibra óptica de propiedad del MEF, (consultar ubicación actual - lamina 04), el movimiento será hasta el área destinada para el cuarto de gabinetes (lamina 03). El piso técnico, acometida eléctrica, tableros eléctricos, los cables, luminarias y aire acondicionado retirados, serán entregados al MEF.
- ✓ Asimismo, el servicio solicitado incluye el retiro del piso técnico actual, desconexión de platinas de cobre (sistema de puesta a tierra) conectadas en los soportes del piso técnico, instalación de un nuevo piso técnico, reconexión de platinas de cobre (sistema de puesta a tierra), reubicación del equipamiento ubicados en los gabinetes comunicaciones existente, garantizando la disponibilidad de los servicios. Los trabajos deben considerar la migración de los equipos que se encuentran en los gabinetes. Para este tipo de trabajos la Entidad proporcionara ventanas de tiempo los fines de semana, las migraciones de equipos que se encuentran en los gabinetes a mover, 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. Adicionalmente el Contratista debe considerar en su Plan de Trabajo la posibilidad de movilizar los gabinetes en ubicaciones temporales (Dentro del misma área a intervenir), reubicar el cableado existente o considerar cableado temporal de requerirse.
- ✓ Para la reubicación de los equipos, se informa que será la Entidad la responsable del apagado y encendido de los servidores, equipos de comunicaciones, aplicaciones y sistema operativo, del backup y/o restauración de la información o software, del procedimiento de encendido y apagado de equipos de TI y de comunicaciones y de pruebas de operatividad de los servicios. El contratista estará a cargo de reubicar físicamente los equipos desde los gabinetes actuales a los nuevos gabinetes.
- ✓ El contratista deberá ofertar la última versión disponible del Hardware y Software del fabricante no se aceptarán versiones beta o similares.
- ✓ 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, para esta etapa el Contratista 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.
- ✓ Todos los cables, tanto eléctricos como de datos, deben ser LSZH de conformidad con la RM N° 175-2008-MEM/DM publicada el 20 de abril del 2008.
- ✓ El Contratista deberá presentar Plan de trabajo y Cronograma de trabajo, el cual debe incluir fechas tentativas de entrega, en un plazo máximo de quince (15) días calendario a partir del día siguiente de la firma del contrato, este plan

debe incluir instalación, configuración de acuerdo a los plazos solicitados, para prever cortes de servicio y horarios para la continuidad del servicio. Plan de Trabajo debe ser aprobado por el MEF, debe permitir viabilizar el retiro del piso técnico actual, la instalación del nuevo piso técnico, garantizando la disponibilidad de los servicios. Asimismo, los trabajos deben considerar la migración de los equipos, que deberán mantenerse operativos o "en caliente". Para este tipo de trabajos la Entidad proporcionará ventanas de tiempo los fines de semana, las migraciones de equipos que se encuentran en los gabinetes existentes, 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. Adicionalmente el Postor debe considerar en su Plan de Trabajo la posibilidad de movilizar los gabinetes en ubicaciones temporales (Dentro del mismo Centro de Ciberseguridad) y cableado temporal de requerirse. Al finalizar el trabajo de mover el equipamiento que se encuentra en los gabinetes, estos deberán quedar limpios, libres de polvo, el cableado estructurado entre los gabinetes y los equipos, deberá están identificado y ordenado.

- ✓ El equipamiento para el Centro de Ciberseguridad del MEF, deberá ser aprobado por la Jefatura de Infraestructura Tecnológica del MEF. La aprobación se realizara durante la etapa de implementación, validando que lo entregado cumpla con lo solicitado en las Especificaciones Técnicas – Anexo A1.
- ✓ El Contratista deberá disponer de las medidas de seguridad necesarias correspondientes al traslado de equipos de cómputo y/o componentes dentro de las instalaciones del MEF.
- ✓ El MEF, posee un sistema backbone interno con 11 cables de fibra óptica multimodo 50/125um de 12 hilos, 04 cables de fibra monomodo de 12 hilos y un panel panel de cobre de 20 puertos categoría 6A. El sistema backbone externo posee un 01 cable de fibra óptica multimodo 50/125um de 12 hilos y 05 cables de fibra óptica monomodo.
- ✓ El diseño propuesto por el contratista, deberá incluir el traslado del sistema bacbone interno y externo ubicados en los gabinetes. Los cables de backbone de F.O. interno y externos, están distribuidos en 04 gabinetes (gabinete 8, 9, 10 y 12). El backbone interno, son enlaces a los cuartos de telecomunicaciones de los pisos del edificio central, el backbone externo, son enlaces a los locales del MEF (Edificio Universal, CCM y Edificio Mercury). En el diseño propuesto por el Contratista, deberá incluir el movimiento del sistema backbone interno y externo, al nuevo gabinete (enlaces), desde la ubicación actual (lamina 04) hasta el Centro de Gabinetes (lamina 03).
- ✓ El contratista deberá reemplazar la bandeja de comunicaciones existente en el área designada para el centro de gabinetes, se deberá emplear bandeja porta cable tipo malla de 100 x 300 mm como mínimo.
- ✓ Se deberá retirar la puerta cortafuego que se encuentra entre el área de operadores y el área del cuarto de gabinetes (lamina 04), también deberá retirar la puerta de vidrio del área de operadores. El contratista deberá instalar la puerta cortafuego que se retiró e instalarla en el ingreso al centro de ciberseguridad.
- ✓ El contratista deberá certificar el cableado estructurado instalados, haciendo uso de los equipos de medición (certificador de cableado estructurado) los cuales deben contar con certificado de calibración vigente. El certificado de calibración vigente deberá ser presentado junto con el plan de trabajo.
- ✓ El Contratista debe diseñar y presentar un plan de capacitación de nivel técnico para el personal de la OGTI que va administrar la solución, el mismo que debe

ser presentado junto con el plan de trabajo. El Contratista bajo cuenta, costo y riesgo se hará cargo de todo lo necesario para llevar a cabo la capacitación.

- ✓ La capacitación debe realizarse como mínimo para siete (07) participantes y será brindada dentro de los primeros noventa (90) días calendarios del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- ✓ 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.
- ✓ Los participantes en el proceso de selección podrán solicitar una visita técnica a las instalaciones del MEF (levantamiento de información), para dimensionar adecuadamente su propuesta. Las visitas técnicas se podrán efectuar desde el día siguiente de la fecha de la convocatoria hasta un día antes de la presentación de propuestas, las mismas que deberán ser solicitadas a la Oficina General de Tecnologías de la Información (OGTI), al correo electrónico procesos-ogti@mef.gob.pe, con el asunto "Proceso de Ciberseguridad". Dichas visitas técnicas deben cumplir con lo mencionado en numeral 16 (SEGURIDAD EN EL TRABAJO) descritos en el presente documento.

Centro de Operaciones de TI del MEF

- ✓ El contratista deberá realizar el equipamiento para el Centro de operaciones de TI, el cual deberá ser supervisado y aprobado por la Oficina de Infraestructura Tecnológica de la OGTI del MEF.
- ✓ El contratista deberá instalar un control de acceso en la puerta de ingreso al centro de operaciones de TI.
- ✓ Se deberá instalar un sistema de video Wall (4x2), el mismo que deberá ser instalado con rack o soportes de montaje que permita la colocación de las pantallas a la altura mínima de 1.45 mts del piso.
- ✓ El contratista deberá ofertar la última versión disponible del Hardware y Software del fabricante no se aceptarán versiones beta o similares.
- ✓ 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, para esta etapa el Contratista 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.
- ✓ Todos los cables, tanto eléctricos como de datos, deben ser LSZH de conformidad con la RM N° 175-2008-MEM/DM publicada el 20 de abril del 2008.
- ✓ El Contratista deberá disponer de las medidas de seguridad necesarias correspondientes al traslado de equipos de cómputo y/o componentes dentro de las instalaciones del MEF.
- ✓ El contratista deberá certificar el cableado estructurado instalados, haciendo uso de los equipos de medición (certificador de cableado estructurado) los cuales deben contar con certificado de calibración vigente. El certificado de calibración vigente deberá ser presentado junto con el plan de trabajo.
- ✓ La capacitación debe realizarse como mínimo para siete (07) participantes y será brindada dentro de los primeros noventa (90) días calendarios del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.

- ✓ El contratista deberá considerar en su diseño la reubicación y distribución de los puntos eléctricos estabilizado y comercial para la implementación del Centro de Operaciones de TI.
- ✓ El contratista deberá considerar en el diseño la reubicación y/o instalación de un nuevo cableado estructurado en categoría 6A.
- ✓ El MEF cuenta con 01 UPS de 100 KVA, el UPS se encuentra en el cuarto de comunicaciones del 1er piso Casa Grace.
- ✓ Todos los conductores de distribución y tomacorrientes serán de cobre con forro de material termoplástico LSHZ y se usará como mínimo el calibre de 4mm2, salvo indicación.
- ✓ El contratista deberá realizar la distribución del cableado eléctrico estabilizado y el cableado eléctrico comercial, para la instalación de los distintos componentes a instalarse en el Centro de Operaciones de TI.
- ✓ Se deberá considerar cableado estructurado para el Video Wall, estaciones de trabajo, control de acceso y demás componentes de la solución propuesta.
- ✓ Se deberá considerar 01 puntos de red categoría 6A, por cada estación de trabajo.
- ✓ 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.
- ✓ Los participantes en el proceso de selección podrán solicitar una visita técnica a las instalaciones del MEF (levantamiento de información), para dimensionar adecuadamente su propuesta. Las visitas técnicas se podrán efectuar desde el día siguiente de la fecha de la convocatoria hasta un día antes de la presentación de propuestas, las mismas que deberán ser solicitadas a la Oficina General de Tecnologías de la Información (OGTI), al correo electrónico procesos-ogti@mef.gob.pe, con el asunto “Proceso de Ciberseguridad”. Dichas visitas técnicas deben cumplir con lo mencionado en numeral 16 (SEGURIDAD EN EL TRABAJO) descritos en el presente documento.

7.2. Características del equipamiento, licencias, servicios

7.2.1. Adquisición de equipamiento y licencias

El Contratista debe entregar el hardware y software requeridos en los **ANEXO A1 y ANEXO B1,** los mismos que deben cumplir como mínimo con las siguientes características técnicas:

Equipamiento para el Centro de Ciberseguridad del MEF	
Descripción	Anexo
Características Técnicas mínimas para el Equipamiento para el Centro de Ciberseguridad del MEF.	A1

Equipamiento para el Centro de Operaciones de TI del MEF	
Descripción	Anexo
Características Técnicas mínimas para el Equipamiento para el Centro de Operaciones de TI del MEF.	B1

7.2.2. Implementación, la etapa de implementación consta del levantamiento de información (traslado de un gabinete de comunicaciones), instalación, configuración, pruebas y puesta en marcha.

El Contratista deberá implementar el equipamiento de hardware y software requeridos en el **Anexo A1** y el **Anexo B1**, 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 (traslado de gabinetes de comunicaciones), instalación, configuración, migración pruebas y puesta en marcha del equipamiento propuesto (hardware y software).

Generalidades:

- ✓ El Contratista debe asegurar la compatibilidad, conectividad e interoperabilidad entre el hardware y software que integre la arquitectura requerida.
- ✓ El MEF será responsable de suministrar el espacio físico donde se alojarán los equipos, para el acondicionamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI.
- ✓ 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, licenciamiento y todo lo que resulte necesario, para dejar completamente habilitado la solución.

Instalación de equipamiento

- ✓ Será de total y exclusiva responsabilidad del Contratista efectuar las tareas necesarias para la puesta en marcha de todo el equipamiento y herramientas proporcionadas (Hardware y Software), todo el cableado y su etiquetado (energía, redes).
- ✓ Los requerimientos específicos se detallan en el anexo A2 y anexo B2.

Equipamiento para el Centro de Ciberseguridad del MEF	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	A2

Equipamiento para el Centro de Operaciones de TI del MEF	
Descripción	Anexo
Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha	B2

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 emitida la Conformidad de la Prestación Principal. Esta garantía debe estar respaldada por el fabricante o su subsidiaria acreditada en el País, al momento de la entrega de los Bienes.
- ✓ 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 equipamiento o hasta que se encuentren vigentes por el fabricante.
- ✓ 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 del Equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI propuestos 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 del Equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI propuestos 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.
- ✓ Todos los componentes del Equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI propuestos, no podrán presentar adulteraciones ni correcciones (por ejemplo: tarjeta madre, fuente, etc.).

9. Reglamentos Técnicos

El contratista 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 contratista 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”
- ANSI/TIA-568-B.1 (Requerimientos Generales).
- ANSI/TIA-568-B.3 (Componentes de Cableado-Fibra Óptica).
- ANSI/TIA-569-B comercial Building Estándar for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechos de soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.
- ANSI/TIA-606A Administration Standard for the Telecomunications Comercial Building dura of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de cableado estructurado.
- J-STD-607B Comercial Building Grounding (Earthing) and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.
- IEEE 802.3an "Physical Layer and Management Parameters for 10GB/S Operation — Type 10GBASE-T.
- International Computer Room Experts Association (ICREA), "Norma Internacional para la Construcción de Centros de Procesamiento de Datos".
- ANSI/BICSI 002-2011, Data Center Design and Implementation Best Practices.
- NFPA 72 National Fire Alarm Code.
- N_FPA 70 National Electrical Code.
- Código Nacional de Electricidad.

11. PRESTACIÓN ACCESORIA: SERVICIO DE CONTINUIDAD OPERATIVA

Se detallan los requerimientos mínimos de la Prestación Accesoria para los bienes ofertados en la Prestación Principal del Anexo A1 y del Anexo B1.

Los requerimientos específicos se detallan en el Anexo A3 y Anexo B3.

Equipamiento para el Centro de Ciberseguridad del MEF	
Descripción	Anexo
Servicio de continuidad operativa	A3

Equipamiento para el Centro de Operaciones de TI del MEF	
Descripción	Anexo
Servicio de continuidad operativa	B3

12. FUNCIONES DEL PERSONAL

Se detalla las funciones del personal:

ITEM PAQUETE 04

Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI del MEF			
Cant.	Personal	Perfil	Actividades
1	Coordinador (Personal Clave)	• Titulado en Administración, Ingeniería de Sistemas o Ingeniería Industrial o Ingeniería electrónica o Ingeniería de las Telecomunicaciones o Ingeniería de Computación y Sistemas. • Certificación de PMP (Project Management Professional). • Experiencia mínima de tres (03) años en servicios de implementación y/o acondicionamiento y/o remodelación y/o construcción de centro de control y/o cuarto de comunicaciones y/o datacenter del personal clave requerido como Coordinador.	• Coordinar la implementación de la solución. • Coordinar con el encargado del área de la OGTI del MEF. • Coordinar con los implementadores de su empresa para el cumplimiento de los objetivos en el tiempo planificado. • Reportar a la OGTI los avances según el cronograma establecido en el plan de trabajo. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana).
2	Implementador I (Personal Clave)	• 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 Industrial.	• Análisis de los detalles técnicos de la tecnología que se va implementar, ya sean especificaciones de hardware, de software, de licenciamiento. • Pruebas de laboratorio, que certifiquen el procedimiento de implementación y las funcionalidades técnicas del producto. • Instalación y configuración de la solución. • Pruebas de la solución implementada. • Elaboración de la documentación de la solución implementada. • Disponibilidad presencial y exclusiva en la entidad (mínimo 8x5 a la semana). • Otros requerimientos asignados por el Jefe de Proyecto.

		• Certificación en ICREA (International Computer Room Experts Associations) y/o ATD (Accredited Tier Designer) y/o CTDC (Certified TIA-942 Design Consultant • Experiencia mínima de tres (03) años en servicios de implementación y/o acondicionamiento y/o remodelación y/o construcción de centro de control y/o cuarto de comunicaciones y/o datacenter del personal clave requerido como Implementador I.	

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.

La contratación del Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI se encuentra detallado en el numeral *"6.1 Descripción y cantidad de los bienes",* habiéndose considerado como un único ítem paquete.

ITEM PAQUETE 04

Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI del MEF	
Descripción	**Cantidad**
Equipamiento para el Centro de Ciberseguridad y el Centro de Operaciones de TI del MEF	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 disgregada 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 Equipamiento del Centro de Ciberseguridad y el Centro de Operaciones de TI.

15.1. Cumplimiento 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.

15.2. 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 perdida 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.

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.

15.3. 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.

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 Secretaria General N° 007-2014-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 del servicio.

La adecuación e 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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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, enlaces web, 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 el Anexo A5 y el Anexo B5 de las mencionadas especificaciones; para tal efecto; deberá presentar también los mencionados formatos (Anexo A5 y Anexo B5) debidamente llenados, indicando la marca, modelo, número de parte del fabricante, 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

- ✓ Documento 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.
- ✓ Documentación donde se indique de manera detallada el peso (kg), espacio (m2), disipación de energía (BTU/hr) y energía eléctrica (watts), de cada uno de los equipos ofertados según corresponda.
- ✓ Declaración Jurada, suscrita por el representante legal del postor ganador, con el compromiso de brindar la garantía de soporte y buen funcionamiento de la totalidad de lo ofertado.

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° 972-2020-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

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 instalará la solución ofertada, será dentro de la ciudad de Lima Metropolitana, sitio Jr. Lampa 277-Cercado de Lima (Centro de Ciberseguridad) y en Jr. Lampa 594-Cercado de Lima (Centro de Operaciones de TI).

19.2. Plazo

Plazo de entrega

El plazo máximo de entrega de los bienes de la prestación principal, es de cincuenta (50) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

Plazo de implementación

El plazo máximo de ejecución de la prestación principal, es de cien (100) días calendario, contabilizados a partir del día siguiente suscrito el contrato.

20. 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.

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, sitio en Jr. Lampa Nº 274 – Cercado de Lima, 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.
- Diseño y actividades a realizar.
- Certificado de calibración vigente del equipo de medición (certificador de cableado estructurado).
- Plan de capacitación de nivel técnico.
- 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.
- Hitos de implementación.
- Diagrama Gantt (Cronograma).
- Horarios de trabajo.
- Documentación del personal clave propuesto tanto del coordinador de la solución e implantador de la solución según lo solicitada en el Equipamiento para el Centro de Ciberseguridad.
- Documentación del personal responsable para las coordinaciones administrativas para llevar el control sobre la prestación accesoria.
- Documentación del personal clave propuesto que brindará la asistencia técnica de la prestación accesoria y deberá contar como mínimo con el perfil y experiencia del personal que será implantador de la solución, según lo solicitado en la solución.
- Responsabilidades y consideraciones.
- Análisis y gestión de riesgos.
    - Identificación de riesgos.
    - Valoración de riesgos.
    - Controles a implementar.
    - Plan de vuelta atrás.

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 cincuenta (50) 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, sitio en Jr.

Lampa N° 274 – Cercado de Lima.
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 implementación de la prestación principal, se deberá entregar un Informe Final, a través de mesa de parles del Ministerio, sitio en Jr. Lampa N° 274 – Cercado de Lima, necesario para que se otorgue la conformidad, donde se indique lo siguiente:

- Trabajos/actividades realizados.
- Actas de avances de los trabajos (si las hubiese).
- Diagramas físicos y lógicos implementados.
- Respaldo de las configuraciones realizadas en todos los equipos ofertados.
- Documento descriptivo de configuraciones de toda la solución ofertada (Hardware y Software).
- Credenciales de todos los dispositivos.
- Inventario de infraestructura suministrada e instalada de hardware, software y licencias.
- Documento de garantías de los bienes entregados.
- Documento 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 los equipos ofertados.
- Conclusiones y Recomendaciones.

Todos los documentos antes mencionados deben ser entregados en formato físico y/o digital a excepción de los respaldos de las configuraciones los cuales serán presentados solo en formato digital.

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.

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 aplicara las siguientes penalidades, de acuerdo con lo dispuesto por el artículo 161° y 163º 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	Incumplimiento de programa o ejecución de trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	Por incumplimiento de participación del personal Cuando se detecte que EL CONTRATISTA envía a un personal clave 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.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida por el MEF, quien notificará a EL CONTRATISTA sobre la falta cometida, permitiéndole que subsane la	10% UIT vigente por cada ocurrencia y por cada día de demora	Informe del área usuaria.

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
	falta en un plazo máximo de veinticuatro (24) horas. Si después de aplicada la penalidad, la falta continúa, se volverá a aplicar la sanción hasta cuando ella sea subsanada.	en subsanar	
4	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.
5	Incumplimiento de los Protocolos Sanitarios	10% UIT vigente por cada ocurrencia	Informe del área usuaria.

25. Responsabilidad por vicios ocultos

Prestación Principal

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

ITEM PAQUETE 04

Solución de Equipamiento para el Centro de Ciberseguridad del MEF	
Anexo A1	Características Técnicas del Equipamiento para el Centro de Ciberseguridad del MEF
Anexo A2	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha
Anexo A3	Servicio de continuidad operativa y transferencia de conocimiento
Anexo A4	Laminas 01, 02, 03, 04, 05, 06, 07 y 08.
Anexo A5	Características Técnicas relevantes del Equipamiento para el Centro de Ciberseguridad

Solución de Equipamiento para el Centro de Operaciones de TI del MEF	
Anexo B1	Características Técnicas del Equipamiento para el Centro de Operaciones de TI del MEF
Anexo B2	Servicio de levantamiento de información, instalación, configuración, pruebas y puesta en marcha
Anexo B3	Servicio de continuidad operativa y transferencia de conocimiento
Anexo B4	Laminas 01, 02 y 03.
Anexo B5	Características Técnicas relevantes del Equipamiento para el Centro de Operaciones de TI

II. Requisitos de calificación

A. Experiencia del Postor en la Especialidad

Para el ítem paquete 04, se debe considerar lo siguiente:

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 500,000.00 (Quinientos Mil con 00/100 Soles), por la venta o suministro 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 bienes similares a los siguientes:

- Venta e implementación de equipamiento para Centro de Control.
- Venta de equipamiento y adecuación de Centro para Control.
- Venta de equipamiento y acondicionamiento para Centro de Control.
- Venta de equipamiento y Remodelación de Centro de Control.
- Venta de equipamiento y Expansión de Centro de Control.
- Venta e implementación de equipamiento para Centro de Datos.
- Venta y adecuación de equipamiento para Centro de Datos.
- Venta de equipamiento y acondicionamiento para Centro de Datos.
- Venta de equipamiento y Remodelación de Centro de Datos.
- Venta de equipamiento y Expansión de Centro de Datos.
- Venta e implementación de equipamiento para Centro de Cómputo.
- Venta y adecuación de equipamiento para Centro de Cómputo.
- Venta de equipamiento y acondicionamiento para Centro de Cómputo.
- Venta de equipamiento y Remodelación de Centro de Computo.
- Venta de equipamiento y Expansión de Centro de Computo.
- Venta e implementación de Data Centers.
- Venta de equipamiento y adecuación de Data Centers.
- Venta de equipamiento y acondicionamiento para Data Centers.
- Venta de equipamiento y Remodelación de Data Center.
- Venta de equipamiento y Expansión de Data Center.
- Venta de equipamiento y Construcción de Centro de Procesamiento de Datos Móvil.
- Venta e implementación de equipamiento para Procesamiento de Datos Móvil.
- Venta y adecuación de equipamiento para Centro Procesamiento de Datos Móvil.
- Venta de equipamiento y acondicionamiento para Centro de Procesamiento de Datos Móvil.
- Venta de equipamiento y Remodelación de Centro de Procesamiento de Datos Móvil.
- Venta de equipamiento y Expansión de Centro de Procesamiento de Datos Móvil.

Acreditación:

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

financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

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

B. Capacidad técnica y profesional

B.1. Experiencia de Personal Clave para el ítem paquete 04:

Requisito

Coordinador

Experiencia mínima de tres (03) años en servicios de implementación y/o acondicionamiento y/o remodelación y/o construcción de centro de control y/o cuarto de comunicaciones y/o datacenter del personal clave requerido como **Coordinador.**

Implementador I

Experiencia mínima de tres (03) años en servicios de implementación y/o acondicionamiento y/o remodelación y/o construcción de centro de control y/o cuarto de comunicaciones y/o datacenter del personal clave requerido como **Implementador I.**

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

EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD

I. Características técnicas

A. Piso Técnico

Se deberá instalar un piso técnico en el centro de ciberseguridad, centro de gabinetes y cuarto de tableros, con las siguientes características:

1. El piso técnico deberá ser fabricado con alma de aglomerado de madera y planchas de aluminio.
2. El piso técnico debe ser para aplicaciones de Data Centers, Cuartos de Telecomunicaciones o Centros de Datos.
3. Espesor de 33 mm como mínimo.
4. Dimensiones de las baldosas 600 x 600 mm como mínimo.
5. Capacidad de carga distribuida mayor o igual a 1,800 kg/m2.
6. Debe contar con una lámina de aluminio en la cara anterior con la finalidad de crear una barrera contra el fuego y la humedad, así como reforzamiento del equipotencial eléctrico para mantener las propiedades de continuidad eléctrica del piso.
7. La altura del piso técnico debe ser de 15 cm (zona A y C) y 10 cm (zona B y D). Cada pedestal debe estar fijado al piso con por lo menos 3 clavos de fijación de acuerdo a las recomendaciones del fabricante.
8. Color de los paneles del tipo técnico: blanco, gris claro o similar.
9. Se deberá proveer 02 chupones para levantar baldosas.
10. El piso técnico deberá ser instalado en las áreas del centro de ciberseguridad, centro de gabinetes, y cuarto de tableros (lamina 02). Las dimensiones son: largo 10.00mts x ancho 8.90mts.
11. Se debe considerar, el retiro del piso técnico existente, e instalación de un nuevo piso técnico según las láminas 01 y 02. El Contratista deberá proponer en su plan de trabajo, el retiro, desconexión del sistema de aterramiento que se encuentra debajo del piso técnico e instalación de un nuevo piso técnico.
12. El plan de trabajo se debe contemplar la desconexión del sistema de aterramiento que está instalado en la estructura de soporte del piso técnico existente, e instalar en la nueva estructura de soporte del piso técnico.

B. Sistema de Iluminación

Se deberá tener las siguientes consideraciones para el sistema de iluminación.

1. Se deberá considerar un mínimo de 23 luminarias (panel cuadrado led), que garanticen como mínimo luz con una iluminación de 500 lux en el plano vertical y 200 lux en el plano horizontal medido desde 1 m por encima del piso terminado en área de trabajo y en cada pasillo.
2. El sistema de iluminación debe ser para toda el área a intervenir, Centro de Ciberseguridad, Centro de Gabinetes y Cuarto de Tableros.
3. Se deberá tomar en cuenta la Norma NFPA75. (Norma para la protección de equipos de cómputo electrónicos y equipos procesadores de datos), la distribución del mobiliario, equipamiento y la deficiencia de iluminación natural, para la distribución de luminarias.

4. Las luminarias se instalarán en el falso techo, se deberá considerar como mínimo 23 luminarias de 0.60 x 0.60mts, las que serán instaladas en las zonas A, B, C y D.
5. No se aceptarán interruptores tipo dimmers.
6. No se reutilizarán luminarias existentes.
7. Todas las luminarias de cada ambiente serán controladas desde un interruptor ubicado al ingreso de cada sala.
8. Se suministrará e instalará equipos automáticos de iluminación de emergencia con un nivel de 450 lux para ser activadas en ausencia del fluido eléctrico con autonomía de 2 horas. Como mínimo se deberá instalar 04 luces de emergencia, la ubicación de las luces de emergencia será 02 en el Centro de Ciberseguridad, 01 en el Centro de Gabinetes y 01 en Cuarto de Tableros.

C. Control de Acceso

Se deberá instalar un sistema de control de acceso para las dos puertas cortafuegos existentes.

1. Capacidad de almacenamiento mínimo de 10,000 huellas digitales.
2. Sensor óptico: (OP5).
3. Debe manejar mínimo 32 zonas horarias.
4. Conectividad a sitios remotos por medio de red (TCP/IP). El dispositivo deberá permitir la conexión con un ordenador mediante TCP/IP, para que pueda recibir todos los datos obtenidos sin necesidad de realizar ninguna configuración en el sistema antes de poder utilizarlo. Además, puede conectarse de forma remota a su control de acceso y presencial.
5. Lector biométrico 1:1
6. Soporte de credenciales móviles, con escaneo QR o NFC.
7. Sensor de huella digital de 500 dpi/nivel de gris 256.
8. Área de detección: 23 x 23 mm.
9. Tiempo de identificación c= 1 seg.
10. Debe proporcionar un solo punto de administración, sin importar los autenticadores que se hayan definido para los usuarios
11. Taza de falsos rechazos (FRR) máxima de 0.001%.
12. Taza de falso emparejamiento (FAR) máxima de 0.0001%.
13. I/O Interface: Ethernet, RS485, RS232, Wiegand, TTL input, Relay, USB.
14. El grado de protección del sistema de control de acceso debe poseer una protección contra sedimentaciones de polvo en el interior y tenga protección contra agua nebulizada (spray), lo cual corresponde al grado de protección IP53.
15. El control de acceso debe ser monitoreable desde la red de datos y la plataforma de gestión.
16. El control de acceso se deberá instalar en las puertas cortafuego del área del centro de ciberseguridad y al centro de gabinetes.
17. Se debe considerar pulsador de salida para ambas puertas cortafuego.

D. Construcción en seco, sellado, pintura de paredes, pisos y puertas

1. Se deberá desmontar la pared interna de drywall que divide la zona B con la zona A, ver (lamina 06).
2. Se deberá realizar tres cerramientos con drywall RF de 12.5 mm, el primer cerramiento se deberá realizar entre la zona A y la zona B (laminas 01 y 07), de 7.60 mts de largo x 2.70 mts de alto, el segundo

encerramiento se deberá realizar en la zona D, de 4.60 mts de largo x 1.60 mts de alto (laminas 01 y 07) y el tercer encerramiento se deberá realizar donde se encuentran las puertas de acceso al cuarto de tableros y centro de gabinetes de 1.20 mts de largo x 160 mts de alto (laminas 01 y 07).

3. Se deberá acondicionar una pared de drywall, en el acceso al centro de ciberseguridad (lamina 07), para la instalación de la puerta cortafuego.
4. Se deberá acondicionar una pequeña pared en el área de acceso al cuarto de tableros y centro de gabinetes, el cual deberá cubrir el tablero eléctrico existente, también se deberá cubrir la apertura que hay entre el techo y el cielo raso existente.
5. Se deberá retirar el techo técnico de baldosas en la zona D (lamina 01). El espacio entre el techo y el falso techo actual es de 0.42mts y el área del falso techo a retirar es de 30 mts2.
6. La estructura metálica de la pared de drywall, estará conformada por perfiles de acero galvanizado, los parantes deberán ser colocados por lo menos cada 0.40 m. y deberán llevar en su interior lana de roca.
7. Las paredes y el techo de las zona A, B, C y D, deberán ser pintadas con pintura resistente al fuego color blanco o “gris-claro-luz de día” para mejorar la iluminación de los ambientes.
8. El Contratista deberá sellar todos los ductos generados por el acondicionamiento del centro de ciberseguridad, centro de gabinetes y cuarto de tableros, adicionalmente deberá sellar dos ductos de acceso existente (lamina 03), con algún sistema corta fuego (tipo firestopping con RF 60 como mínimo). También se deberán sellaran los ductos generados para la instalación de la montante vertical eléctrica.
9. El Contratista deberá retirar circuitos, toma eléctrica y puntos de cableado estructurado. Los cables eléctricos de las luminarias e interruptor a retirar de las zonas A, B, C y D (lamina 01), vienen del tablero de distribución comercial del quinto piso. El Contratista deberá considerar bandeja porta cable tipo malla y/o tubería metálica EMT, para la instalación de las nuevas luminarias, interruptores, circuitos eléctricos, control de acceso, video Wall, detección de incendio, Workstation y demás componentes a implementar. El cableado estructurado, viene del cuarto de telecomunicaciones del quinto piso (02 cables UTP) y del centro de ciberseguridad (cables UTP).
10. El contratista también deberá pintar el piso del Centro de Ciberseguridad con resinas epóxicas color ladrillo, dicha pintura debe cubrir los muros perimetrales hasta la altura del piso técnico.
11. El contratista deberá utilizar las dos puertas cortafuego existente en el área del centro de datos, en ambas puertas se deberá instalar el control de acceso.
12. Se deberá retirar la puerta cortafuego que se encuentra entre el área de operadores y el área del cuarto de gabinetes (lamina 04).
13. El contratista deberá retirar la puerta de vidrio del área de operadores (lamina 04).
14. El contratista deberá instalar la puerta cortafuego que se retiró e instalarla en el ingreso al centro de ciberseguridad.

E. Falso Cielo Raso

Implementación de un falso cielo raso en la zona del centro de ciberseguridad con las siguientes características técnicas como mínimo:

1. Baldosas de 0.60 x 0.60 mts.

2. Color blanco.
3. Contenido de material reciclado no mayor de 60%.
4. Clasificación: ASTM E 1264 Tipo XX modelo G.
5. Resistencia térmica: 1/2” = hasta R-0.45.
6. Propagación de llama: 20.
7. Espesor total mínimo: 12 mm.
8. La altura mínima del falso cielo respecto al piso será de 2.40 mts.
9. La implementación del falso cielo raso será: Centro de Ciberseguridad.
10. El falso cielo raso deberá ser instalado en las zonas B y D (lamina 01), del centro de ciberseguridad (lamina 07). Las dimensiones son: largo 9.60mts x ancho 5.8mts.

F. Sistema de Aire Acondicionado

1. El sistema de enfriamiento deberá estar basado como mínimo con 03 equipos de aire acondicionado tipo Split Decorativo, los cuales serán proporcionados e instalados por el contratista. Cada equipo debe contar con un condensador y un evaporador (lamina 03).
2. La capacidad de cada uno de los equipos de aire acondicionado deberá ser como mínimo de 32000 btu/h.
3. El voltaje de cada uno de los equipos de aire acondicionado, deberá ser de 220V/60Hz o 380V/60Hz trifásicos.
4. El tipo del compresor deberá ser del tipo rotativo.
5. El flujo del aire deberá ser mayor a 1200 m3/h.
6. El contratista deberá realizar los trabajos necesarios para que los equipos queden fuertemente fijados a la pared.
7. Los equipos de aire acondicionado deberán tener su propio control remoto.
8. Todas las tuberías de cobre deberán ser debidamente forradas con su respectivo aislante térmico.
9. La ubicación de las 03 unidades condensadoras será: 02 unidades en centro de gabinetes y 01 unidad en centro de ciberseguridad (lamina 03).
10. El contratista será responsable de la construcción del soporte, dicho soporte deberá contar con una escalera de acceso tipo gato y sistema de drenaje para mantenimiento.
11. Las tuberías deberán ser de cobre con diámetros seleccionados de acuerdo a las recomendaciones del fabricante.
12. El contratista deberá instalar los puntos de drenaje y puntos de interconexión eléctrica para las unidades evaporadoras y condensadoras.
13. Vacío y carga del equipo con refrigerante ecológico R-410.
14. Los condensadores de los equipos de aire acondicionado existente, se encuentran instalados en una plataforma metálica, la misma que esta colindante a la puerta de acceso al Cuarto de Tableros. Se requiere instalar una nueva plataforma metálica al costado de la existente, para la instalación de los 03 condensadores nuevos (lamina 06). La distancia lineal, entre los condensadores y evaporadoras de los dos equipos de aire acondicionado existentes, es de 17.50 mts aproximadamente.
15. Se deberá considerar el desmontaje de los condensadores y evaporadores de los dos equipos de aire acondicionado existentes.

G. Gabinete de comunicaciones

1. Se requiere de 05 gabinetes de comunicaciones de 800 mm ancho x 1100 profundidad, 42 RU, como mínimo.
2. Se deberán instalar 05 gabinetes de comunicaciones en el área designada centro de gabinetes, en estos gabinetes se deberá reubicar los equipos, patch panel, enlaces de los gabinetes actuales, la distribución será la siguiente:
    - Gabinete 01: 18 equipos entre router, media converter y radio enlaces.
    - Gabinete 02: 17 patch panel de cobre y bandeja de fibra óptica.
    - Gabinete 03: Switch Core, distribución, borde y equipos diversos.
    - Gabinete 04: Switch Core, distribución, borde y equipos diversos.
    - Gabinete 05: Equipos y cableado estructurado del acondicionamiento del centro de ciberseguridad.
    - Gabinete 06: Reserva.
3. Los gabinetes propuestos deberán ser para soporte de equipos electrónicos adaptables y escalables que permita una adecuada distribución del cableado eléctrico y de datos. Los gabinetes deben incluir como mínimo una (01) puerta delantera con cerradura, perforada por lo menos al 77%, dos (02) puertas traseras con cerradura divididas y perforadas al 77% como mínimo, dos (02) pares de rieles de montaje de 19”, cuatro (04) paneles laterales divididos con pestillo de bloqueo, panel superior extraíble sin herramientas, ruedas y pies niveladores. Además, debe permitir la instalación de dos (02) PDU de altura completa y administrador de cables. Debe incluir kit de unión, tuercas enjauladas y tornillos que permitan su instalación. Los sistemas centrales deben ser ensamblados en fábrica, listos para la instalación de equipos electrónicos suministrados por el cliente.
4. Los gabinetes deberán cumplir con las siguientes certificaciones como mínimo:
    • EIA-310
    • UL2416
    • RoHS
5. El marco deberá soportar como mínimo 1350 kg carga de peso estático, 1022 kg de peso dinámico (sin transito) de carga.
6. Incorporará cuatro (4) ruedas giratorias y pies niveladores accesibles desde la parte superior. Las patas niveladoras deberán ser accesibles cuando se instale equipo de TI en el marco.
7. Los rieles de montaje deberán estar construidos con chapa de acero de calibre 14, rieles de 19”, doblados 5 veces para máxima rigidez, regulación de ajuste final en posición mediante sistema deslizante, identificación de Unidades en los 4 montantes 19" con fijación por grabación laser dirección 1 a 42U y 42 a 1U (2 sentidos).
8. Debe incluir un destornillador / adaptador para el ajuste de las patas niveladoras.
9. Debe poseer barra a tierra vertical en cobre 99.99% pureza bajo normativa CE o UL. Todos los equipos instalados en el gabinete instalados en el gabinete deberán aterrarse a la barra a tierra vertical con cable TW 12 AWG.
10. Los gabinetes deberán estar conectado al sistema de aterramiento (debajo del piso técnico).
11. Las puertas deberán ser desmontables sin herramienta y reversibles.

12. Puerta gabinete delantera, con manija confort Giratoria Pivotante, cuadro interior rigidizado soldado, Kit de continuidad eléctrica (para garantizar punto común de tierra con el gabinete), nivel de perforación debe ser 75% como mínimo, grosor mínimo de la puerta 0.9 mm.
13. Puerta gabinete 42U posterior plana, con apertura (doble puerta), con aireación (perforada), con manija confort Giratoria Pivotante, Kit de continuidad eléctrica (para garantizar punto común de tierra con el gabinete), nivel de perforación debe ser 75% como mínimo, grosor mínimo de la puerta 0.9 mm.
14. El panel superior se podrá retirar sin herramientas e incluirá dos (02) espacio de tamaño mínimo de 152 mm x 100 mm ubicados en la parte delantera y trasera del panel para la entrada o salida de cables.
15. Deberá admitir el montaje de 02 PDUs (debe incluir adaptadores). Uno para cada lado del gabinete, los cuales serán alimentados de manera que haya un circuito independiente para alimentar cada PDU (ramal A y ramal B)

H. Unidad de Distribución de Energía (PDUs)

1. Se deberá considerar 02 PDUs para cada gabinete nuevo y 02 PDUs para el gabinete existente (gabinete 7).
2. 230Voltaje, 50/60 Hz, 32 A.
3. Conector: IEC60309 2P+G.
4. 25 salidas IEC60320 C13 y 04 salidas IEC60320 C19 para los PDU de 32 A.
5. Monitoreable a través de WebBrowser, SNMP, HTTP, Telnet. Además deberá soportar monitoreo a la salida de: Kwh, W, VA, PF, V y A.

I. Conmutador de Trasferencia Automática

1. Se deberá suministrar 14 Conmutadores de Trasferencia Automáticas.
2. Entrada:
   - Doble alimentación eléctrica, 220V, 60 Hz, monofásico.
   - Conectores de entrada tipo IEC-C20 x 2.
   - Voltaje de entrada 150 – 300 Vac.
3. Salida:
   - Deberá tener como mínimo 06 tomas C14.
   - Capacidad de sobrecarga 125% por 30 minutos.
   - Tiempo de conmutación típico <6ms, <11ms como máximo.

J. Sistema de Video Wall (3x2)

1. Deberá tener rack o soporte de montaje que permita la colocación de las pantallas a la altura mínima de 1.00 mts del piso, micro ajustable que permita una alineación precisa. Fabricado en acero de carbono, montaje con liberación rápida de pantalla que facilite el mantenimiento, con pintura electroestática. Se deberá reforzar el interior de la pared de drywall, para la instalación de los rack o soporte de montaje.
2. Resolución de 1920 X 1080.
3. Tecnología de panel LED.
4. Tamaño mínimo de los monitores: 55 pulgadas.
5. Relación de contraste: 1000:1 contraste dinámico, como minimo.
6. Conectividad: DVI-I (D Sub Common), Display Port 1.2 (1), HDMI 2.0 (2), stereo Mini Jack, USB 2.0 x 1.
7. Montaje tipo VESA.

8. Con Fuente de alimentación auto voltaje de 100 – 240VAC, de 50 o 60 Hz, consume típico 180 W, y un máximo de 297 W.
9. Condiciones de operación: Temperatura de 0° a 40° C, humedad relativa de 10 a 80 % sin condensación.
10. Con certificación FCC, CE, UL o equivalente.
11. Accesorios: Manuales de instalación, garantía, cable power, cable HDMI, Cable DVI, control remoto con baterías incluidas.

K. Controlador de Video Wall

1. Procesador: 6 núcleos, 12 subprocesos, frecuencia del procesador 3,70 Ghz.
2. RAM de 16 GB.
3. Sistema Operativo compatible con la solución de Video Wall propuesta.
4. El paquete de software deberá contar con licencia de usuarios, opciones incluidas: Captura de red ilimitada, hasta 12 decodificadores IP de strems HD.
5. Se deberá considerar 01 fuente redundante y 01 disco duro redundante.
6. El controlador de video Wall, deberá generar múltiples formas de visualización. Se deberá configurar y guardar las visualizaciones y colocarlas en el video wall según se requiera.

L. Workstation

1. Procesador de última generación, con 6 núcleos, 12 subprocesos, de 5.00 GHz Frecuencia, como mínimo.
2. RAM de 32 GB. DDR4-2400, LPDDR3-2133, como mínimo.
3. Tarjeta de video, resolución 4096 x 2160, conectores Dual conexión DVI-I y HDMI, memoria 2 G, como mínimo.
4. Sistema Operativo compatible con la solución de video Wall propuesta.
5. Placa del sistema 7x 1.2, DVI, VGA, HDMI, como mínimo.
6. Disco duro rápido y grande (SSD 512 GB), como mínimo.
7. Deberá contar con licenciamiento del sistema operativo. Así como teclado y mouse.
8. Conectividad con el controlador del Video Wall opciones incluidas: Captura de red, hasta 12 decodificadores IP de streams HD.
9. Monitor de 24 pulgadas IPS, 1920 X 1080, HDMI / DP / miniDP / USB / Audi. Brillo 250 cd/m2, contraste 1000:1, relación de aspecto 16:9, tiempo de respuesta 6ms, autovoltaje.
10. 10/100/100 Ethernet.
11. Soporte doble brazo giratorio, montaje universal, altura regulable Min. 10.0 cm. Max 42.0 cm, inclinación 30° giro lateral 360° independiente, soporte hasta 16 Kg, fabricado en aluminio.
12. Cantidades: 09 Workstation y 18 monitores como mínimo.

M. Plataforma de Gestión

1. Plataforma unificada de seguridad

1.1 La plataforma deberá soportar la unificación perfecta del sistema de control de acceso, cámaras IP, todo bajo una sola plataforma.

1.2 Las aplicaciones de interfaz de usuario de la plataforma deberán presentar una interfaz unificada de seguridad para la administración, la configuración, el monitoreo y la generación de informes de los sistemas control de acceso y de los dispositivos periféricos asociados.

1.3 Presentación de mapa gráfico dinámico. Se desea visualizar el sistema de control de acceso, cámaras IP.
1.4 Las comunicaciones con software de control de acceso deberán realizarse a través de una red IP, y no deberán soportar tareas administrativas.
1.5 La plataforma deberá ser capaz de integrarse con el sistema de Video Wall.
1.6 Debe permitir consolidar y ejecutar todas las actividades de seguridad en una sola aplicación.
1.7 Debe permitir privilegios de seguridad avanzados y creación de Particiones: que permita definir quién tiene acceso a su sistema de seguridad física y lo que pueden hacer mediante privilegios individuales y la creación de particiones en el sistema. El sistema deberá soportar el control total del acceso del usuario y del operador.
1.8 Debe permitir encriptación de extremo a extremo: las comunicaciones entre las aplicaciones del cliente, aplicaciones del servidor, y controladores de puerta estén protegidos al activar la encriptación a lo largo del sistema.
1.9 Debe permitir la gestión y tratamiento de los niveles de amenazas: mediante respuestas rápidas a las amenazas que perciba, y restrinja el acceso según los niveles de amenaza pre configurado basado en sus políticas corporativas de seguridad.

2. Servidor
2.1 Sistema operativo para Workstation.
2.2 Procesador 3.3 Ghz,8M Cache, 4C/4T turbo (80W), como mínimo.
2.3 RAM 32 GB. DDR4-2400.
2.4 Disco duro: 1TB 7.2 RPM SATA 6 Gbps 3.5in Cableado.
2.5 DVD+/-RW, SATA, Interno.
2.6 PCI Slots: 1 x Gen3 slot (x16), 2X Gen3 slot (x4), 1 x PCI
2.7 Hasta 1 TB de almacenamiento total.
2.8 Gigabit Ethernet LAN 10/100/1000.
2.9 4 x USB 2.0 5 x USB 3.0, 1 x USB 3.1.
2.10 1x DisplayPort.
2.11 Teclado y mouse

N. Mobiliario

1. Se deberá implementar mobiliario para el Centro de Ciberseguridad, el cual contará con lo siguiente:

1.1 09 estaciones rectas de melamine con cajoneras movibles, como mínimo (tener en consideración que cada Workstation va a contar con 2 monitores).
1.2 09 sillones ergonómicos, como mínimo.

2. Las estaciones rectas de melanine se instalarán en el centro de ciberseguridad, en las cuales se colocarán los Workstation y monitores de 24” (se requiere dos brazos articulados por estación), que tiene como finalidad servir de herramientas de trabajo de los operadores, estas también contarán con dos cajas para toma eléctrica y una caja toma datos. Los operadores contarán con una silla ergonómica para el confort de los operadores durante el periodo de trabajo.

3. Estaciones rectas
3.1 Medidas 1.20 x 0.70 x 0.75 metros.

3.2 Estructura metálica electro soldado de perfil cuadrado, con acabado de pintura de aplicación electroestática.
3.3 Tablero de melanina color blanco de 25 mm.
3.4 Tapacantos de PVC de 03mm termo fusionados.
3.5 Cajoneras movibles.
3.6 04 Caja de tomas metálica, (03 troqueles) fabricado en PL LAF 1/32.
3.7 Canaleta pasa cable.

4. Silloneras ergonómicos
   4.1 Araña de aluminio.
   4.2 Garruchas de Nylon PU.
   4.3 Mecanismo neumático basculante, con ajuste de tensión y regulable en reclinación.
   4.4 Brazos regulables en altura.
   4.5 Peso máximo 120-150 Kg.

5. El locket deberá ser construido en melamine color blanco de 25mm, con tapacantos de PVC de 03mm termo fusionado. El locket deberá tener 08 comparticiones con puerta y chapa. La distribución de los compartimientos será distribuida en dos niveles. Las medidas del locket 1.50 mts x 1.20 mts x 0.40 mts. El locket deberá estar asegurado a la pared.

O. Sistema Eléctrico Estabilizado y Comercial

1. El contratista será el responsable de realizar el diseño del Sistema de electricidad estabilizada y comercial.
2. El contratista deberá considerar en su diseño, el equipamiento instalado en los gabinetes existentes (lamina 04) que se encuentran en el área a intervenir, más lo solicitado en la Implementación del Centro de Ciberseguridad.
3. El MEF cuenta con dos UPS de 60 KVA cada uno, los UPS se encuentra en el cuarto eléctrico del Sótano (lamina 05).
4. Se debe garantizar que los 06 gabinetes (05 gabinetes nuevos y 01 gabinete existente), cuente con sus propios circuitos de energía y tomas eléctricas necesarias para la conectividad total de los equipos de comunicaciones y demás dispositivos. Los gabinetes deberán contar con dos circuitos eléctricos estabilizados independientes. Un circuito eléctrico del primer tablero de distribución de energía estabilizada (UPS) y un circuito eléctrico del segundo tablero de distribución de energía estabilizada (UPS).
5. Se deberá considerar, 02 PDUs por cada gabinete nuevo y 02 PDUs para el gabinete reubicado. Además, se deberá considerar 02 tomacorrientes dobles con espiga a tierra del tipo hospitalario, con NEMA 5-15R, con placa de acero inoxidable y 01 tomacorriente doble universal, con NEMA 5-15R con placa de acero inoxidable, por cada estación de trabajo (09 unidades).
6. Se deberá considerar 14 Conmutadores de Transferencia Automáticos (ATS / STS).
7. Se deberá suministrar 70 cables de poder de C13 – C14 14 AWG, como mínimo de 2 metros de longitud.
8. Se deberá instalar el cableado eléctrico sobre una red de bandejas galvanizadas en caliente porta cables de dimensión mínima 50mm x 250 mm, con facilidades de ventilación natural (conectado a tierra en todo su recorrido) para el ordenamiento de todos los cables eléctricos de los servidores, y para los cables eléctricos de las tomas dobles eléctricas

donde sea necesario, además se podrán utilizar sistemas de bandejas debajo del piso técnico, dependiendo del diseño del Contratista. Esta bandeja será exclusivamente para cableado eléctrico horizontal.

9. Se deberá considerar tubería galvanizada para las 03 acometidas eléctricas (sótano al quinto piso).
10. Los tableros a instalarse, así como los accesorios necesarios deberán cumplir con las normas del Código Nacional de Electricidad.
11. Los interruptores termo magnéticos deberán ser automáticos, de disparo interno que permitirá la desconexión de la fase del circuito al sobrecargarse o cortocircuitarse una sola línea.
12. Todos los conductores de distribución y tomacorrientes serán de cobre con forro de material termoplástico LSHZ y se usará como mínimo el calibre de 4mm2, salvo indicación.
13. Los conductos de sección igual o superior al calibre 4mm2 serán cableados.
14. Se deberá considerar como mínimo 2 tableros de distribución de energía estabilizada (UPS), la distribución de los circuitos será la siguiente:
    Primer tablero de distribución de energía estabilizada (UPS):
    - Primer PDU (ramal A) para los 06 gabinetes.
    - Circuito eléctrico para tomacorrientes Workstation (tomacorrientes A).
    - Sistema extinción de incendio.
    - Sistema control de acceso.

    Segundo tablero de distribución de energía estabilizada (UPS)
    - Segundo PDU (ramal B) para los 06 gabinetes.
    - Circuito eléctrico para tomacorrientes Workstation (tomacorrientes B).
    - Sistema de video Wall.

    De tal manera que se obtenga un sistema paralelo distribuido. El sistema de detección de incendio debe tener una batería de respaldo de 07AH de capacidad. El sistema de Control de Acceso debe tener integrado batería de respaldo de mínimo 06 horas de autonomía.
15. Un Tablero de Distribución de energía comercial, se conectarán los 03 equipos de aire acondicionado Split decorativo, tomacorrientes comerciales y luminarias (ubicados en el centro de ciberseguridad, centro de gabinetes y cuarto de tableros).
16. Cada tablero debe incluir un medidor de energía digital que permita ver como mínimo: voltaje, amperaje, consumo de energía y frecuencia. Se debe incluir todos los accesorios para que quede en correcto funcionamiento.
17. El Contratista deberá conectar a tierra todos los equipos, canalizaciones metálicas, gabinetes, estructuras metálicas y piso técnico instalado.
18. Se deberá emplear bandeja porta cable del tipo malla, hasta la ubicación final de los gabinetes (lamina 03 – Centro de Gabinetes), por donde se instalarán dos circuitos eléctricos para cada gabinete (05 gabinetes nuevos y 01 gabinete existente). Las medidas mínimas de la bandeja serán de 50mm x 250mm.
19. Los equipos a instalarse, así como los accesorios necesarios deberán cumplir con las normas del Código Nacional de Electricidad y la correspondiente norma NEC 250.
20. Los conductores de protección de cobre para la puesta a tierra deben estar acorde con la NTP 370.053. En ningún caso la sección nominal del conductor de puesta a tierra podrá ser menor a 10 mm2.
21. El contratista deberá conectar a tierra todos los gabinetes y equipos dentro de ellos.

22. El MEF cuenta con una barra a tierra TMGB, la misma que está instalada en el Sótano. En el área destinada para el centro de gabinetes, está instalada una barra de tierra TGB (lamina 04). La barra de tierra TGB, cuenta con espacio para realizar nuevas conexiones.
23. Todas las tuberías serán metálicas del tipo EMT, elaboradas según las normas lTl NTEC-Perú.
24. El radio mínimo de curvatura será superior a 6 veces el diámetro exterior de la tubería, no permitiéndose en ningún caso ángulos menores de 90°.
25. Las uniones entre tuberías serán por medio de uniones de fábrica.
26. Las tuberías serán continuas entre cajas y serán colocadas en lo posible en línea recta o en su efecto con curvas suaves.
27. Las uniones de tuberías a caja se efectuaron con "conexiones a caja" del mismo material que la tubería. Todas las salidas, empalmes y conexiones de conductores eléctricos, para las derivaciones de la instalación eléctrica se harán con cajas metálicas de fierro galvanizado pesado.
28. El contratista deberá retirar las acometidas eléctrica estabilizada y comercial, y los tableros eléctricos que actualmente están dando servicio al equipamiento del entro de cómputo (gabinetes).
29. Todos los elementos retirados de la acometida eléctrica, tableros eléctricos y circuitos de derivación desmontados, serán entregados al MEF.

P. Cableado estructurado

Se deberá considerar cableado estructurado para el Video Wall, estaciones de trabajo, control de acceso y demás componentes de la solución propuesta.
Se deberá considerar 04 puntos de red categoría 6A, por cada estación de trabajo.
Se debe proveer e instalar canales de cobre categoría 6 A entre Gabinetes (diagrama de distribución de gabinetes en la Lamina 08 del Anexo A4), según lo siguiente:

- Acorde al diagrama de la lámina 08, en los gabinetes G 01 se instalarán equipos router, media converter y radio enlaces, en el gabinete G 02 cableado backbone (enlaces internos y externos), en el gabinete G 03 y G 04 equipos switches Core, distribución y borde, en el G 05 equipamiento del centro de ciberseguridad, cableado estructurado de Workstation y componentes del acondicionamiento y en el gabinete G 06 gabinete de reserva.
- 24 puntos de cableado categoría 6 A desde cada uno de los gabinetes G 01, G 02, G05 y G06 a los gabinetes de G 03 y G 04, ambos extremos deberán tener patch panels y patch cords de 10 pies de longitud.
- 24 puntos de cableado categoría 6 A desde gabinetes G 03 al Gabinete G 04, ambos extremos deberán tener patch panels y patch cords de 10 pies de longitud.
- 24 puntos de cableado categoría 6 A desde el gabinete G 01 al gabinete G 02, ambos extremos deberán tener patch panels y patch cords de 10 pies de longitud.

Todos los componentes del cableado estructurado deberán ser de categoría 6 A, todos los componentes serán de un solo fabricante, deberán cumplir con los parámetros de IEC60332-3 (se aceptará IEC60332-3C o IEC60332-

33 o IEC60332-3A), LEC 60754 e IEC 61034 (se aceptará también el cumplimiento de la norma IEC 601034 en reemplazo de la norma IEC 61034), no se aceptará ningún cable de tipo CM o CMX.,
Como mínimo se deberá considerar los siguientes componentes:

1. Cable par trenzado categoría 6 A, deberá ser apantallado (FTP, F/UTP o U/FTP) los conductores deben ser de cobre solido calibre entre 22 a 24 AWG.
2. Modulo Jack RJ45 categoría 6 A, deberá cumplir con la norma TIA/EIA 568-C.2.
3. Patch panels con 24 Jacks RJ45 Categoría 6 A, deberá incluir 24 Jacks Categoría 6 A.
4. Patch Cords Categoría 6 A, deberá tener conectores RJ-45 a ambos extremos, se deberá suministrar un patch cords de 10 pies o de 3 mts de longitud y un patch cord de 3 pies o 1 mts de longitud, por cada punto instalado, los patch cords deberán ser instalados a través de los ordenadores horizontales, la chaqueta del patch cord deberá ser con bajo nivel de humo y libre de alógeno (LSZH) y deberá cumplir con los parámetros de 1EC60332-1.
5. Se deberá considerar como mínimo de 04 ordenadores horizontales por cada gabinete (05 gabinetes nuevos y 01 gabinete reubicado) de 88 mm x 483 x 332 mm, con cubierta trasera delantera con bisagra, el ordenador horizontal deberá ser de plástico ABS.

Sistema de Canalización, para el sistema de canalización de datos, voz y video, se deberá considerar bandeja porta cable tipo malla galvanizada en caliente. La bandeja porta cable deberá ser fabricado con hilos de acero soldados juntos y plegados en sus formas finales.
La malla de la bandeja porta cable deberá ser de 50 mm x 250 mm como mínimo, garantizando en todo momento un 40 % de crecimiento. Las bandejas deberán ser instaladas, suspendidas en techo y/o debajo del piso técnico, según la distribución del equipamiento propuesto (cableado estructurado, cámaras IP, control de acceso y demás componentes de la solución propuesta). También se deberá emplear bandeja porta cable tipo malla de 100 x 300 mm como mínimo, para reemplazar la bandeja existente en el área designada para el centro de gabinetes.
Para el sistema de canalización del sistema eléctrico, se deberá considerar bandeja porta cable tipo malla galvanizada en caliente. La bandeja porta cable deberá ser fabricado con hilos de acero soldados juntos y plegadas en sus formas finales.
La malla de la bandeja porta cable deberá ser de 50 mm x 250 mm como mínimo, garantizando en todo momento un 40 % de crecimiento. Las bandejas deberán ser instaladas, suspendidas en techo y/o debajo del piso técnico, según la distribución del equipamiento propuesto (cableado eléctrico a gabinetes, Workstation, cámaras IP, control de acceso y demás componentes de la solución propuesta).

Para el recorrido de preferencia debe ser por debajo del piso técnico y/o falso techo. Todas las bandejas (cableado estructurado y cableado eléctrico), deben estar conectadas en todo su recorrido al sistema de puesta tierra existente (barra TGB), se deberá emplear cable de cobre desnudo de 16 mm2 como mínimo.

Switch administrable de 48 puertos, se deberá considerar la instalación de un switch 10/100/1000 de 48 puertos, en capa 3. El switch deberá contar con fuente redundante (02 fuentes de poder), los cuales podrán ser reemplazados en caliente, sin necesidad de apagar el switch. Todos los 48 puertos deberán soportar Power over Ethernet Plus (PoE+).
El switch deberá contar con 04 puertos uplinks de 10Gb cada uno.

Q. Detección de Incendios – Sistema de Monitoreo

1. El sistema de detección de incendios que se implemente deberá estar aprobado y normado por códigos nacionales e internacionales, como son:
   1.1 NFPA 72 National Fire Alarm Code.
   1.2 NFPA 70 National Electrical Code.
   1.3 Código Eléctrico Nacional.
2. El servicio de implementación del sistema de seguridad contra incendios deberá considerar, como mínimo, con los siguientes componentes:
   2.1 Panel de control para detectores inteligentes.
   2.2 Batería de respaldo de 07AH de capacidad.
   2.3 Detectores fotoeléctricos inteligentes.
   2.4 Anunciador audible y luminoso.
3. Detectores fotoeléctricos de humo.
4. Anunciador audible y luminoso.
5. Sistema de Monitoreo (Cantidad 01)
   5.1 Accesible a través de un explorador Web.
   5.2 Creación de gráficos a partir de datos.
   5.3 Soporte 2 sensores y hasta 5 sensores universales.
   5.4 Sensor de humedad y temperatura.
   5.5 Sensor de punto de condensación.
   5.6 Sensor de temperatura.
6. Registro de eventos.
7. Todos estos componentes deben estar integrados en un Sistema de Administración del Centros de Ciberseguridad, que consiste en un appliance que permita ver todo el estado y funcionamiento de los distintos sensores.
8. Asimismo, el Sistema debe ser capaz de ver e integrar todos los componentes del Centro de Ciberseguridad. Como mínimo UPS, aires acondicionados y poder ser visualizados en el video wall.
9. Las áreas a proteger por el Sistema de Detección de Incendios serán: Centro de Ciberseguridad, Cuarto de tableros y Centro de gabinetes.

R. Cámaras IP

1. Se requiere cámaras de monitoreo de tipo bullet, que deberán cumplir lo siguiente:
2. Características de la Cámara de Monitoreo cantidad: 05 unidades
   - Bloqueo de cámaras.
   - Aprobaciones: CE,FCC Part 15 Clase A, En la lista de UL,VCCI.
   - Procesador de imágenes que genera imágenes de una resolución de hasta 1280x1024, color de 24 bits y hasta 30 fotogramas por segundo.

- Detección del movimiento a través de la cámara. LED de actividad, que indica el estado de alimentación y grabación del módulo, estas características son opcionales.
- Sensor de movimiento a través de cambio de pixeles.
- Accesible a través de un explorador Web.
- Acciones configurables.
- Registro de eventos.
- Notificación de fallas.
- Informes de historial de incidentes.

3. Todas las cámaras IP deberán estar integrados en un Sistema de Administración de Infraestructura de Centros de Ciberseguridad que consiste en un appliance que permita ver todas las cámaras y grabar las secuencias de imágenes en un disco duro que permita por lo menos 6 meses de grabación.
4. Asimismo, el Sistema debe ser capaz de ver e integrar todos los componentes del Centro de Ciberseguridad. Como mínimo UPS (opcional), aires acondicionados y cámaras.
5. El proveedor debe configurar alertas y el medio de envío.
6. Debe permitir hasta 3 niveles de usuarios como mínimo.
7. Debe permitir el monitoreo de salas que se encuentren físicamente separadas.
8. Compatible con BMS lo cual será opcional.
9. La cantidad de cámaras requeridas son cinco (05), las ubicaciones son:
    - Cuarto de tableros.
    - Puerta de ingreso al Centro de Gabinetes.
    - Puerta de ingreso al Centro de Ciberseguridad.
    - Centro de Gabinetes.
    - Centro de Ciberseguridad.

ANEXO A2
EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD

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

a) Levantamiento de Información

1. Se debe realizar el levantamiento de información, con el fin de poder realizar el traslado de los gabinetes de comunicaciones en el Centro de Ciberseguridad.
2. Se debe realizar el levantamiento de información para el retiro del piso técnico existente, instalación de un nuevo piso técnico, sistema eléctrico, sistema de aire acondicionado, detección de incendios, control de acceso, video Wall y mobiliarios.

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. Se debe incluir la migración del equipamiento ubicado en los gabinetes de comunicaciones existentes, estos equipos deberán mantenerse operativos o "en caliente". Para este tipo de trabajo la Entidad proporcionará ventanas de tiempo los fines de semana, adicionalmente el contratista debe considerar en su Plan de Trabajo, el traslado de un gabinete existente.
3. Se deberá realizar la desconexión del sistema de aterramiento, que est instalado en la estructura de soporte del piso técnico existente, e instalar el sistema de aterramiento en la nueva estructura de soporte del piso técnico.
4. Se debe implementar un sistema de control de acceso de tipo biométrico mediante huella dactilar, escaneo QR o NFC y credencial móvil, que incluya cerradura electromagnética.
5. Se debe sellar los ductos de ingreso al Centro de ciberseguridad, con algún sistema corta fuego (tipo firestopping con RF 60 como mínimo).
6. Se debe retirar circuitos y tomas eléctricos y de cableado estructurado, luego se deberá nivelar y pintar las paredes de material noble y Drywall con pintura resistente al fuego color blanco o “gris-claro-luz de dia”.
7. Se debe pintar el piso del Centro de Ciberseguridad con resinas epóxicas color ladrillo, dicha pintura debe cubrir los muros perimetrales hasta la altura del piso técnico.
8. Se debe instalar un sistema de aire acondicionado (Split decorativo) para el área del Centro de Ciberseguridad (01 equipo) y para el área de Centro de Gabinetes (02 equipos). Las unidades de interiores y de condensación estarán diseñadas para un funcionamiento silencioso y comodidad de los operarios.

9. Se debe montar en cada uno de los 06 gabinetes de comunicaciones, 02 PDUs.
10. Se debe instalar un bloque de 06 pantallas y el controlador del video wall.
11. Se debe realizar una configuración especial de pantallas o monitores profesionales que se sincronizarán para mostrar contenidos, usando como interfaz un controlados y Workstation como equipos de trabajo que enviarán el contenido.
12. Se debe instalar y configurar el controlador para video Wall, el cual será Pre-cargado con el software de administración de contenido.
13. Se debe reforzar la pared de drywall donde se instalará los racks o soporte de montaje que permita la colocación de las pantallas a la altura mínima de 1.00 mts del piso, micro ajustable que permita una alineación precisa.
14. Se debe instalar y configurar el controlador del Sistema de Video Wall.
15. Se debe instalar como mínimo 09 workstation con 18 monitores de 24 pulgadas.
16. Se debe unificar la Plataforma de Gestión perfectamente al sistema de control de acceso y sistema de administración de video bajo una sola plataforma.
17. Se debe integrar la plataforma de gestión con el sistema de Video Wall.
18. Se debe configurar la Plataforma de Gestión, de tal forma que permita consolidar y ejecutar todas las actividades de seguridad en una sola aplicación.
19. Se debe crear privilegios de seguridad avanzados y creación de Particiones: que permita definir quién tiene acceso a su sistema de seguridad física y lo que pueden hacer mediante privilegios individuales y la creación de particiones en el sistema.
20. Se debe configurar la Plataforma de Gestión, de tal forma que permita la gestión y tratamiento de los niveles de amenazas: mediante respuestas rápidas a las amenazas que perciba, y restrinja el acceso según los niveles de amenaza pre configurado basado en sus políticas corporativas de seguridad.
21. Se debe instalar y configurar el servidor de la Plataforma de Gestión.
22. Se debe instalar como mínimo 02 tableros de distribución de energía estabilizada y 01 tablero de distribución de energía comercial, en el cuarto de tableros del quinto piso del edificio central (costado del centro de ciberseguridad).
23. Se deberá instalar tres acometidas eléctricas; dos acometidas eléctricas para los dos tableros de distribución de energía estabilizada, y una acometida eléctrica para el tablero de distribución de energía comercial. Las acometidas eléctricas se instalaran desde el cuarto eléctrico N° 2 del sótano del edificio principal. El recorrido de las acometidas eléctricas se realizara, desde el sótano hasta el quinto piso del edifico principal. También se deberá proveer llaves ITM para la conexión a los tableros ubicados en el cuarto eléctrico N° 2, el tablero eléctrico del cuarto eléctrico N° 2, cuenta con instalación al sistema de puesta a tierra. Para el cálculo del recorrido de las acometidas eléctricas, se deberá considerar la siguiente altura: sótano 3.60mts, primer piso y mezanine 5.60mts, segundo piso 3.15mts, tercer piso 3.20mts cuarto piso 3.45mts y quinto piso 3.00mts.Para el cálculo del recorrido de las acometidas se deberá considerar la siguiente altura: sótano 3.60mts, primer piso y mezanine

5.60mts, segundo piso 3.15mts, tercer piso 3.20mts cuarto piso 3.45mts y quinto piso 3.00mts.

24. Los nuevos tableros eléctricos se instalaran dentro del cuarto de tableros, el mismo que se encuentra al costado del Centro de Ciberseguridad.
25. Se debe instalar el cableado eléctrico horizontal hasta la ubicación final de los gabinetes y estaciones de trabajo.
26. Se debe instalar el sistema de cableado estructurado para todos los componentes ofertados, tales como; Video Wall, Workstation, Sistema de Control de acceso, Sistema de Detección de Incendios, Cámaras y demás componentes que lo requiera.
27. Se deberá instalar un switch 10/100/100 de 48 puertos, en capa 3 para todo el equipamiento del centro de ciberseguridad. El switch 10/100/100 de 48 puertos deberá ser instalado en el gabinete 05 – Centro de Ciberseguridad.
28. Se debe instalar y configurar un sistema de detección de incendios.
29. Se debe documentar todos los procedimientos realizados en la implementación del centro de ciberseguridad.

c) Pruebas y puesta en marcha

1. Las inspecciones y pruebas se realizarán una vez culminadas la implementación del Acondicionamiento del Centro de Ciberseguridad.
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 y el MEF ejecutarán en forma conjunta los procedimientos de inspección.
4. Los procedimientos de inspección incluirán como mínimo:

    - Detalle de las actividades a realizar por el MEF, 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 el MEF o el CONTRATISTA.

5. Cualquier defecto notificado por el MEF 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 el MEF.

ANEXO A3: PRESTACIÓN ACCESORIA

EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD

CONTRATACION DEL SERVICIO DE CONTINUIDAD OPERATIVA

1. Consideraciones generales

- Este servicio cubrirá todo el hardware y software ofertado.
- La prestación de este servicio es a partir del día siguiente de la conformidad de la prestación principal, y tendrá una duración 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.
- Las labores técnicas a realizar sobre la solución se llevarán a cabo en el lugar donde esta se encuentra instalada.
- 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.
- 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, por vía telefónica o por mensajería instantánea. 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 atendido 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.

2.1.2. Soporte técnico

- El Servicio de Soporte Técnico debe brindarse en modalidad 24x7x365, incluyendo fines de semana y feriados.
- 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. En caso de falla, inoperatividad o problema el contratista se encargará de corregir el mal funcionamiento o el riesgo tecnológico en los sistemas propuestos (Plataforma de Gestión, Video Wall, control de acceso, Equipos de Aire Acondicionado, Detección de Incendios, Sistema Eléctrico). De ser necesario, debe gestionar con el fabricante incidentes, fallas problemas o requerimientos presentados según el nivel de complejidad.
- 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 a los sistemas instalados 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.

2.2. Características y actividades del servicio de mantenimiento preventivo

- El mantenimiento preventivo se realizará sobre los bienes adquiridos, incluyen 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 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. 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 del equipamiento instalado.
- Debe ser brindada dentro de los primeros noventa (90) días calendario del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- Debe estar enfocada en las funcionalidades a nivel de administración, soporte y monitoreo de la solución instalada.

- Debe estar dirigida para siete (07) personas pertenecientes a la OGTI. Cada una de las personas debe recibir una capacitación mínima de doce (12) horas.
- La frecuencia debe ser mínimo tres (03) veces a la semana, de lunes a viernes (fuera del horario de oficina) y sábados.

2.3.1. 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.

2.3.2. 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, 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.

2.4. 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.

2.4.1. 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 y presentación de los entregables mensuales.

2.4.2. Servicio de Mantenimiento Preventivo:

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

- Informe del 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.
  -

2.4.3. Servicio de Capacitación

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 capacitación, según detalle:

- Documento de Capacitación.
  - Nombre del personal
  - Temario
  - Cantidad de horas de la capacitación brindada.
  - Certificados de los participantes de la capacitación.

3. Nivel de Servicio

Se requiere un soporte técnico ante fallas o problemas con la solución propuesta (Sistema de Iluminación, Control de Acceso, Sistema de Aire Acondicionado, Unidad de Distribución de Energía, Sistema de Video Wall, Controlador de Video Wall, Workstation, Plataforma de Gestión, Sistema Eléctrico Estabilizado y Comercial, Detección de Incendio – Sistema de Monitoreo). El contratista deberá entregar su procedimiento de atención cumpliendo con lo siguiente.

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

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Incidencias Corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo en la solución	**Alto**	**Tiempo de respuesta:** 30 minutos **Tiempo de solución:** 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.
	Medio	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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.
	Bajo	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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 o incidentes presentados en producción sobre la solución que no afecten a usuarios, pero reducen la calidad de servicio de la solución.

TABLA N° 01: Servicio de Soporte Técnico de Incidencias

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

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Requerimiento Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	**Medio**	**Tiempo de Respuesta** 2 horas **Tiempo de Solución** 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 soluciona 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.

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 I 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 como mínimo en control de acceso, sistema de video wall, controlador de video Wall, plataforma de gestión. 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 implementados. 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.

Personal de capacitación: Será la persona encargada de brindar la capacitación en el manejo de la solución ofertada al personal designado por la OIT.
El personal para la capacitación debe estar avalado por la marca para brindar la capacitación oficial.

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 requerimientos 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	Incumplimiento De Programa O Ejecución De Trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	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 del servicio (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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
5	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:

THM = 24 x 90 = 2,160 horas

THE = 4+3 = 7 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%

Rango de UPTIME	Penalidad(1)
>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 el Centro de Ciberseguridad del quinto piso del edificio principal.

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

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.

9.2. 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, 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 Capacitación, se realizará un solo pago, luego de emitida la conformidad, previa presentación del Documento de Capacitación.
- Para el Servicio de Mantenimiento Preventivo, se realizará en seis (6) pagos en partes iguales, luego de emitida la conformidad previa presentación del informe por la realización del servicio.

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 perdida 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.
El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria 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 dictadas por los sectores y autoridades competentes, así como las que se dicten durante el periodo de prestación del servicio.

La adecuación e 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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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

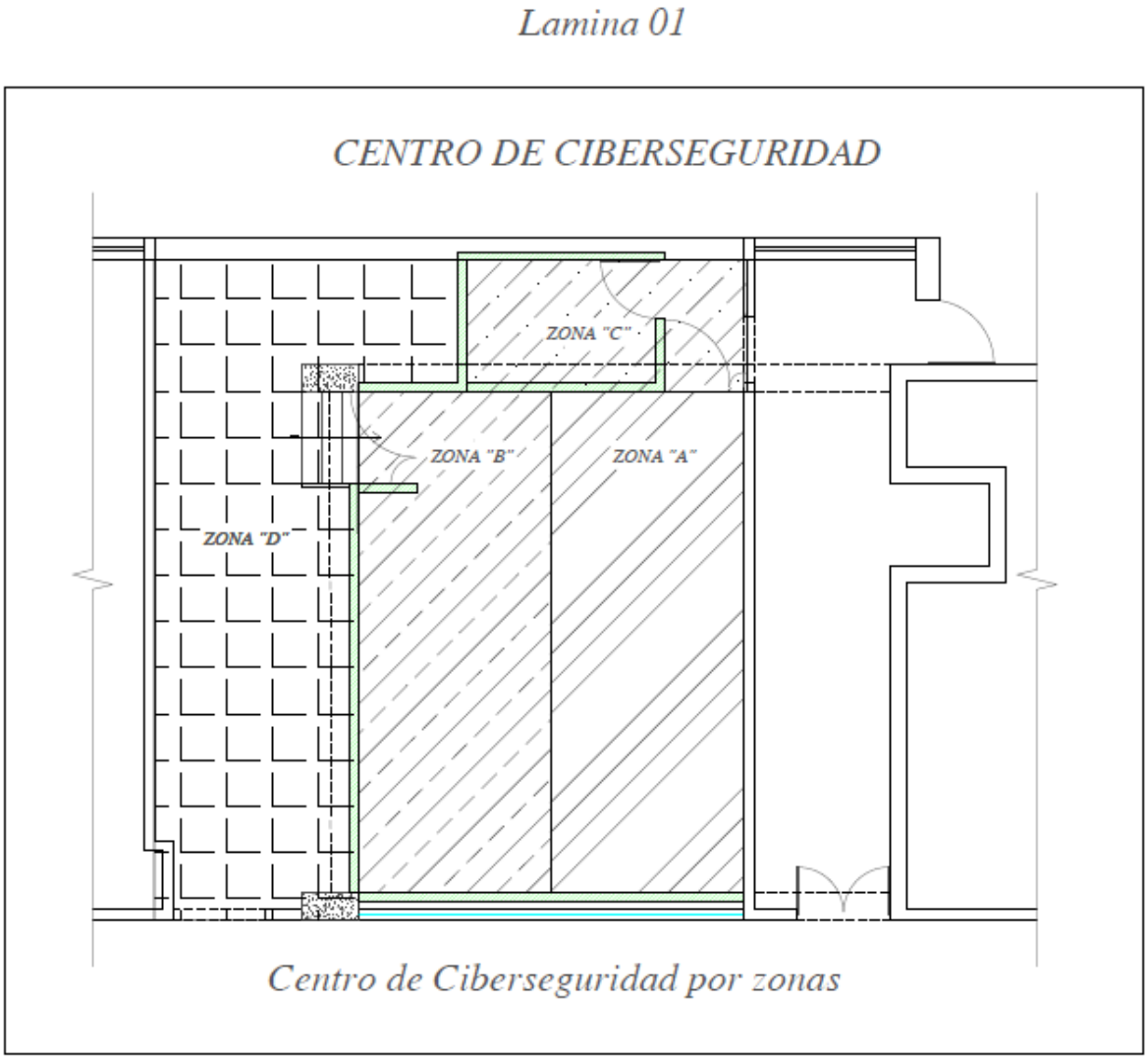
Como parte del servicio, el contratista pudiera tomar conocimiento de la información de la plataforma tecnológica y de los sistemas de información del MEF. Si este fuera el caso, esta información es reservada, por lo tanto, el contratista y todo su personal deberá mantener la confidencialidad de la misma. 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.

ANEXO A4

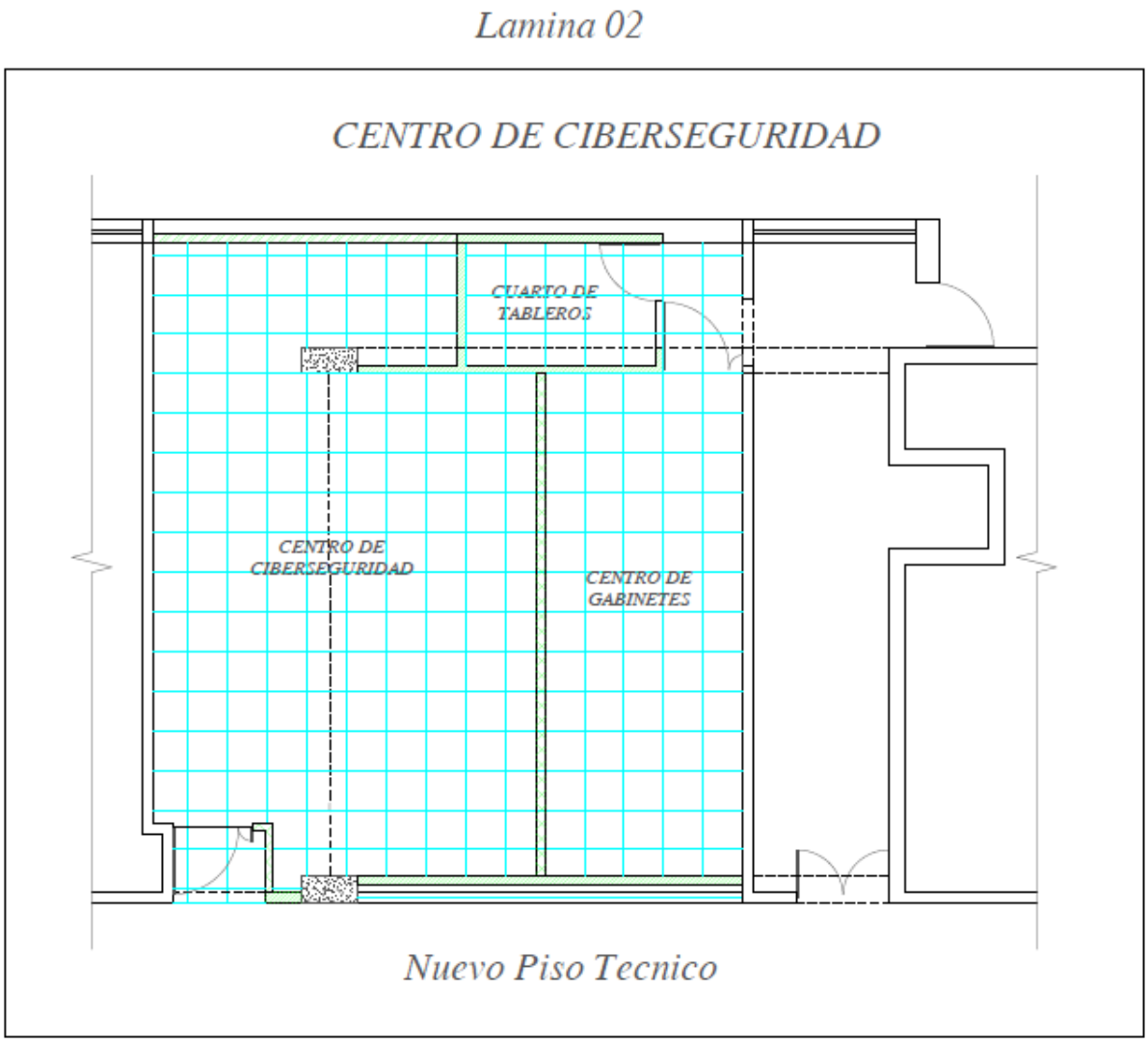
EQUIPAMIENTO PARA EL CENTRO DE CIBERSEGURIDAD

Se adjuntan planos de la ubicación donde se implementará el Centro de Ciberseguridad del MEF.

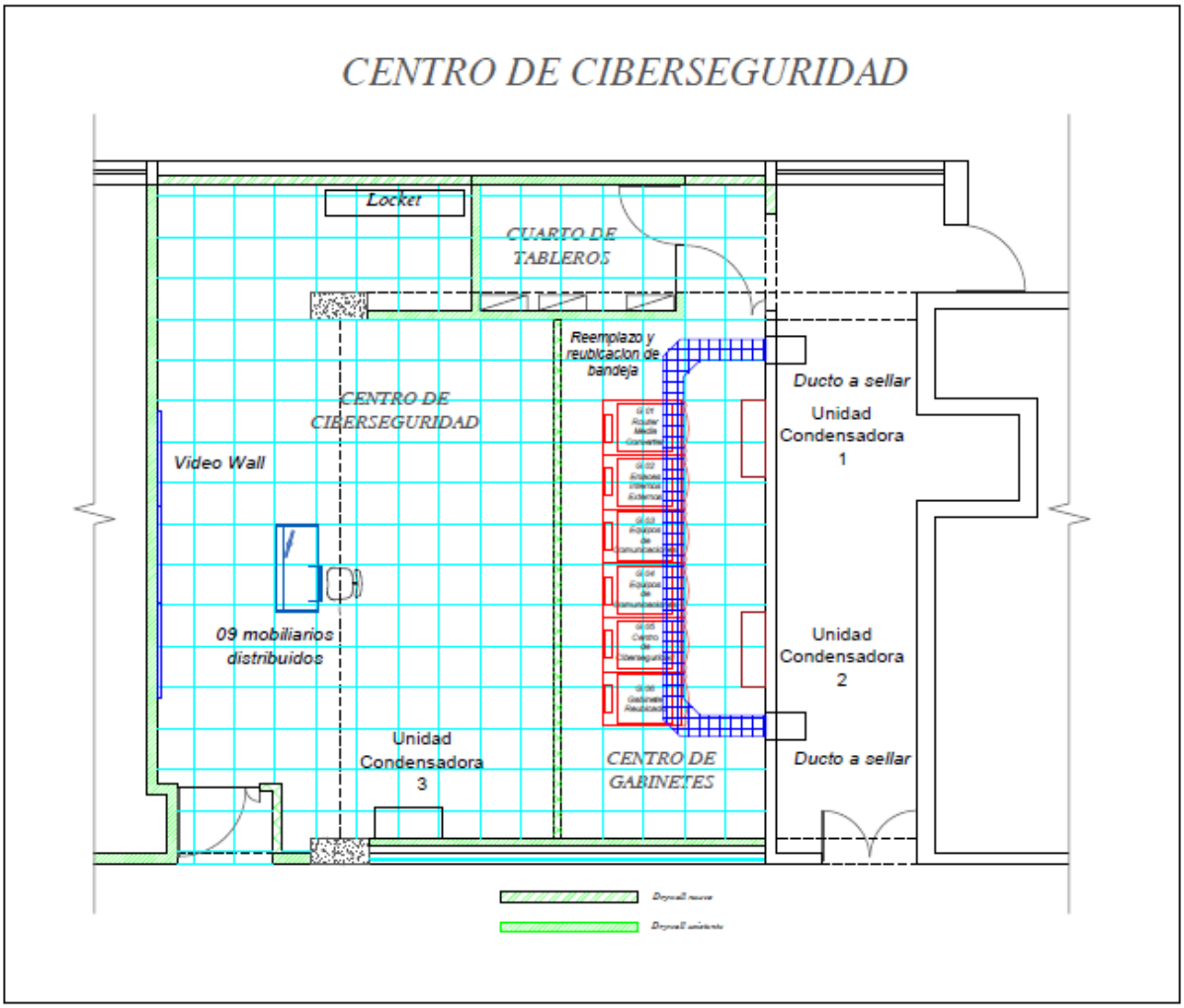
Lamina 01: Plano del Centro de Ciberseguridad dividido por zonas



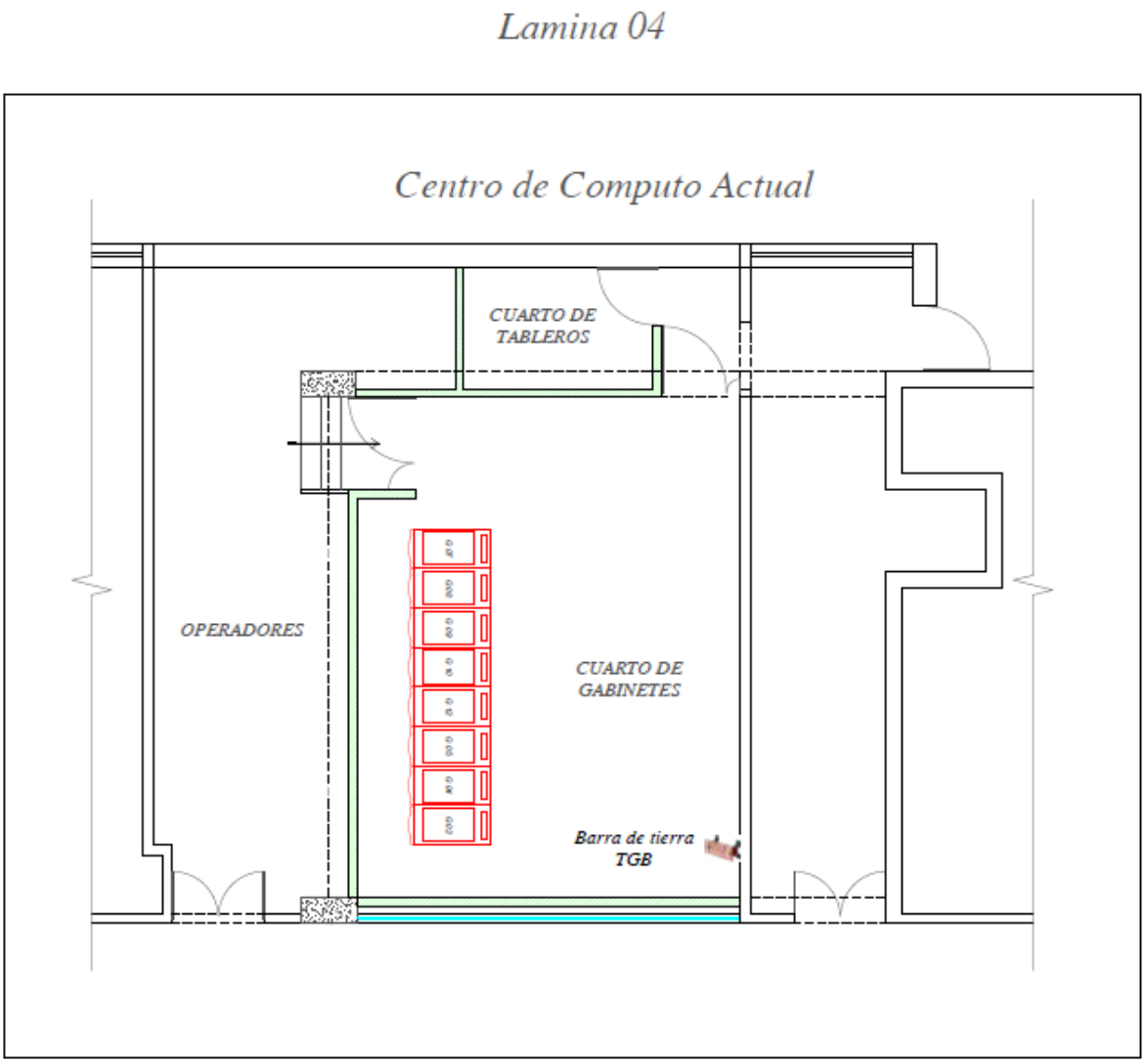
Lamina 02: Piso técnico nuevo



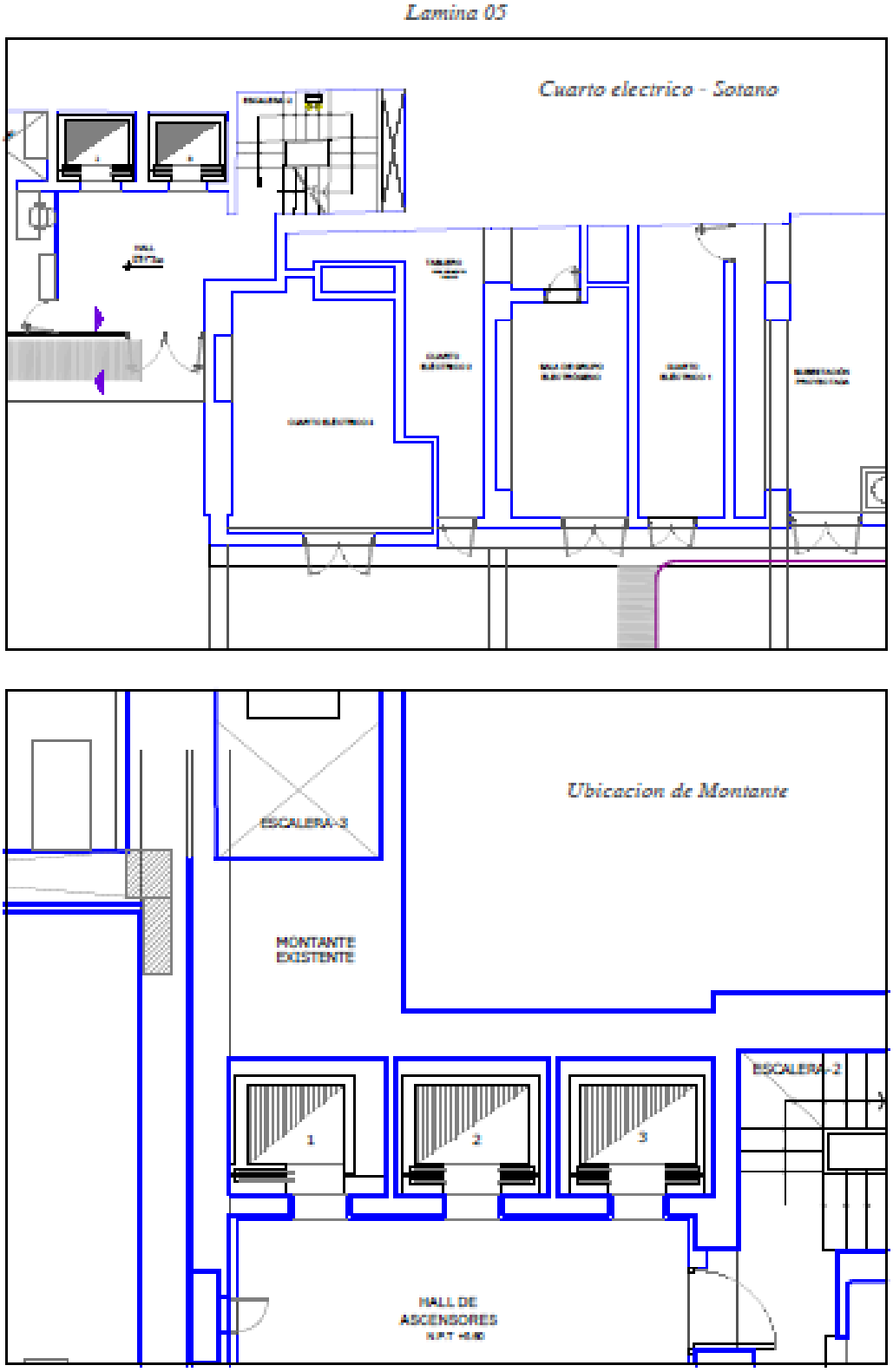
Lamina 03: Centro de Ciberseguridad Final



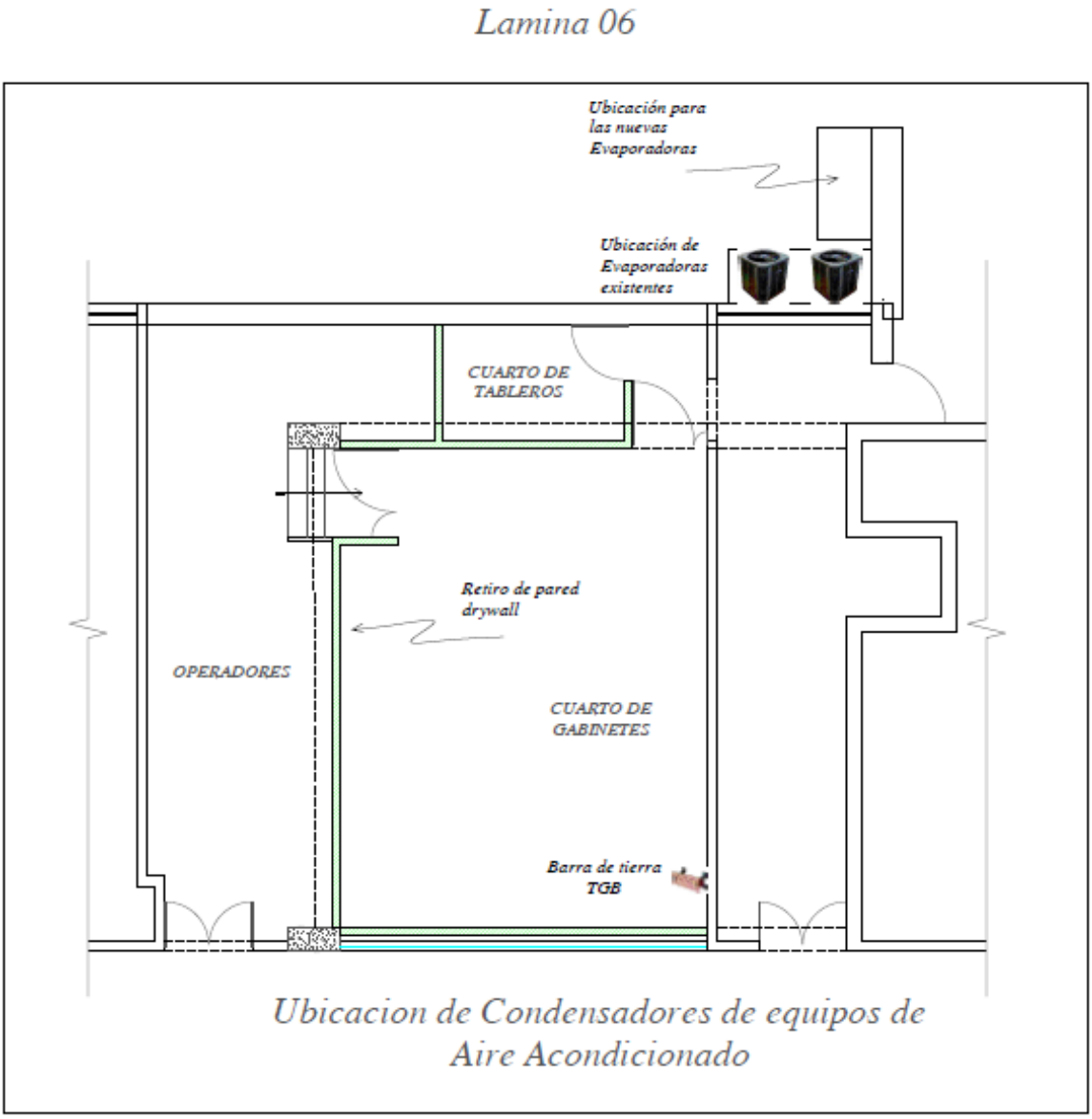
Lamina 04: Estado actual del Centro de Cómputo



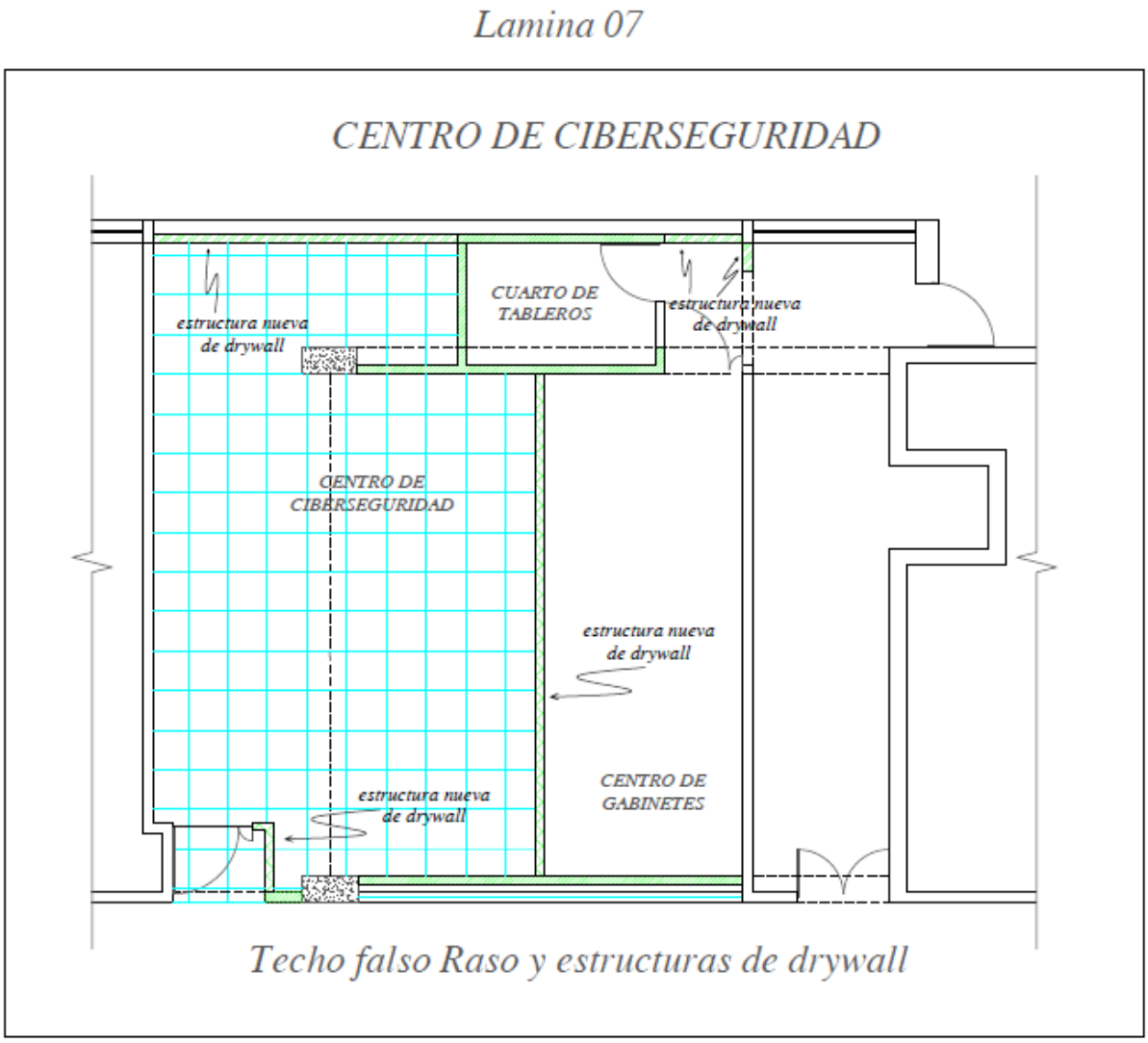
Lamina 05: Ubicación de los cuartos eléctrico – Sótano



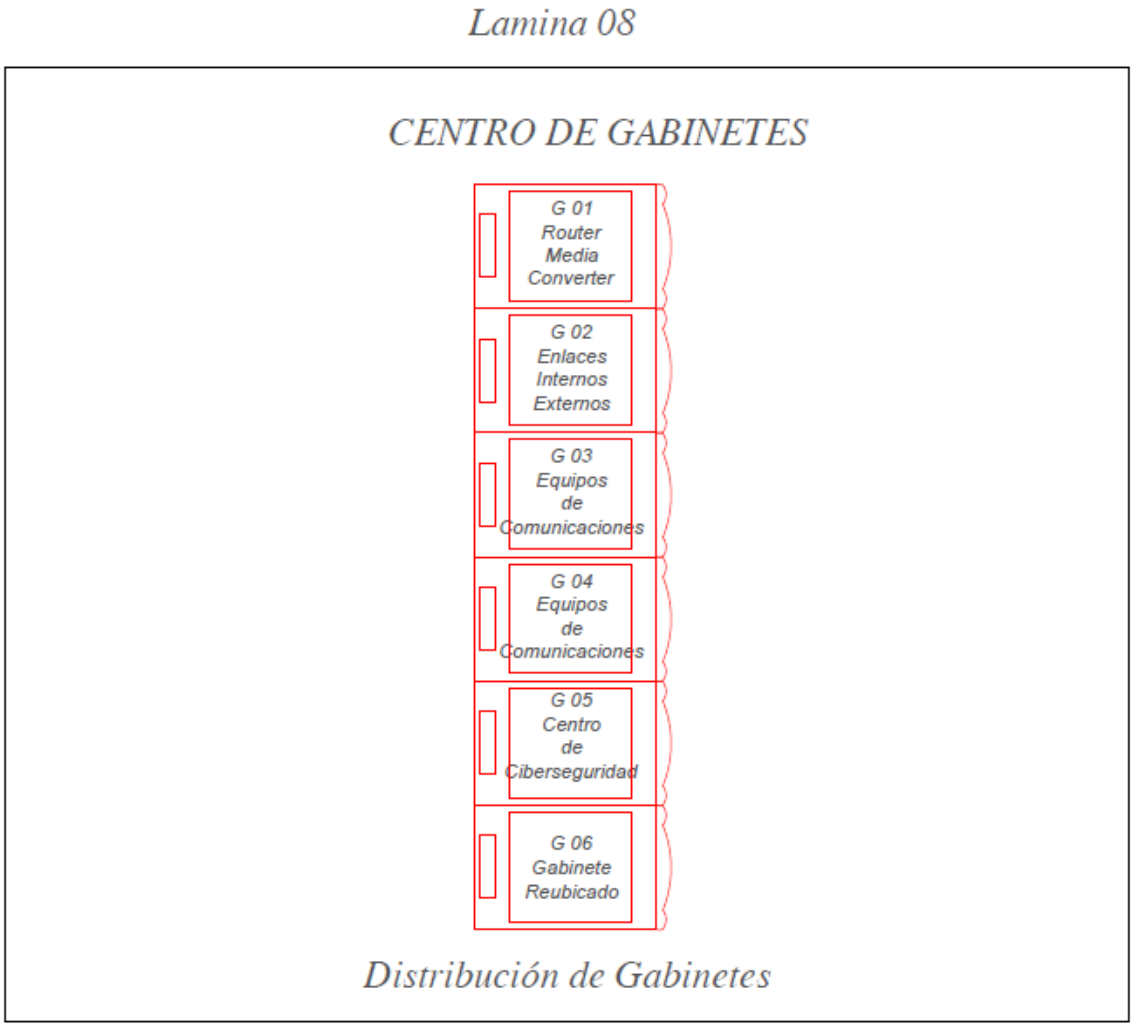
Lamina 06: Diagrama ubicación de Condensadores



Lamina 07: Diagrama Techo Falso y estructuras de drywall



Lamina 08: Diagrama de distribución de gabinetes en centro de gabinetes



Gabinete G 02
Enlaces Internos y Externos

42	Ordenador
41	
40	Panel 24 Cat 6A - G 03
39	Panel 24 Cat 6A - G 04
38	Ordenador
37	
36	Panel 24 Cat 6A - G 01
35	
34	
33	
32	
31	
30	
29	
28	
27	
26	
25	
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

Gabinete G 01
Router, Media Converter

42	Ordenador
41	
40	Panel 24 Cat 6A - G 03
39	Panel 24 Cat 6A - G 04
38	Ordenador
37	
36	Panel 24 Cat 6A - G 02
35	
34	
33	
32	
31	
30	
29	
28	
27	
26	
25	
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

Gabinete G 04
Equipos de Comunicaciones

42	Ordenador	42
41		41
40	Panel 24 Cat 6A - G 01	40
39	Panel 24 Cat 6A - G 02	39
38	Ordenador	38
37		37
36	Panel 24 Cat 6A - G 05	36
35	Panel 24 Cat 6A - G 06	35
34	Ordenador	34
33		33
32	Panel 24 Cat 6A - G 03	32
31		31
30		30
29		29
28		28
27		27
26		26
25		25
24		24
23		23
22		22
21		21
20		20
19		19
18		18
17		17
16		16
15		15
14		14
13		13
12		12
11		11
10		10
9		9
8		8
7		7
6		6
5		5
4		4
3		3
2		2
1		1

Gabinete G 03
Equipos de Comunicaciones

42	Ordenador	42
41		41
40	Panel 24 Cat 6A - G 01	40
39	Panel 24 Cat 6A - G 02	39
38	Ordenador	38
37		37
36	Panel 24 Cat 6A - G 05	36
35	Panel 24 Cat 6A - G 06	35
34	Ordenador	34
33		33
32	Panel 24 Cat 6A - G 04	32
31		31
30		30
29		29
28		28
27		27
26		26
25		25
24		24
23		23
22		22
21		21
20		20
19		19
18		18
17		17
16		16
15		15
14		14
13		13
12		12
11		11
10		10
9		9
8		8
7		7
6		6
5		5
4		4
3		3
2		2
1		1

Gabinete G 06
Gabinete Reubicado

42	
41	Ordenador
40	Panel 24 Cat 6A - G 03
39	Panel 24 Cat 6A - G 04
38	
37	Ordenador
36	
35	
34	
33	
32	
31	
30	
29	
28	
27	
26	
25	
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

Gabinete G 05
Centro de Ciberseguridad

42	
41	Ordenador
40	Panel 24 Cat 6A - G 03
39	Panel 24 Cat 6A - G 04
38	
37	Ordenador
36	
35	
34	
33	
32	
31	
30	
29	
28	
27	
26	
25	
24	
23	
22	
21	
20	
19	
18	
17	
16	
15	
14	
13	
12	
11	
10	
9	
8	
7	
6	
5	
4	
3	
2	
1	

ANEXO A5

Equipamiento para el centro de ciberseguridad

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.**
Equipamiento para el centro de ciberseguridad					
A. Piso Técnico					
1. Capacidad de carga distribuida mayor o igual a 1,800 kg/m2.					
C. Control de Acceso					
1. Soporte de credenciales móviles, con escaneo QR o NFC.					
G. Gabinete de comunicaciones					
1. Se requiere de 05 gabinetes de comunicaciones de 800 mm ancho x 1100 profundidad, 42 RU, como mínimo					
2. Los gabinetes deberán cumplir con las siguientes certificaciones como mínimo: • EIA-310 • UL2416 • RoHS					
H. Unidad de Distribución de Energía (PDUs)					
1. 25 salidas IEC60320 C13 y 04 salidas IEC60320 C19 para los PDU de 32 A.					

2. Monitoreable a través de WebBrowser, SNMP, HTTP, Telnet. Además deberá soportar monitoreo a la salida de: Kwh, W, VA, PF, V y A.				
J. Sistema de Video Wall (3x2)				
1. Resolución de 1920 X 1080.				
2. Tecnología de panel LED.				
3. Relación de contraste: 1000:1, contraste dinámico.				
4. Conectividad: DVI-I (D Sub Common), Display Port 1.2 (1), HDMI 2.0 (2), stereo Mini Jack, USB 2.0 x 1.				
5. Montaje tipo VESA.				
6. Con Fuente de alimentación auto voltaje de 100 – 240VAC, de 50 o 60 Hz, consume típico 180 W, y un máximo de 297 W.				
7. Condiciones de operación: Temperatura de 0° a 40° C, humedad relativa de 10 a 80 % sin condensación.				
8. Con certificación FCC, CE, UL o equivalente.				
K. Controlador de Video Wall				
1. Procesador: 6 núcleos, 12 subprocesos, frecuencia del procesador 3,70 Ghz				
2. RAM de 16 GB.				
3. Sistema Operativo compatible con la solución de Video Wall propuesta.				
4. Se deberá considerar 01 fuente redundante y 01 disco duro redundante.				
L. Workstation				
1. Procesador de última generación, con 6 núcleos, 12 subprocesos, de 5.00 GHz Frecuencia, como mínimo.				
2. RAM de 32 GB. DDR4-2400, LPDDR3-2133, como mínimo.				
3. Tarjeta de video, resolución 4096 x 2160, conectores Dual conexión DVI-I y HDMI, memoria 2 G, como mínimo.				
4. Sistema Operativo compatible con la solución de video Wall propuesta.				
M. Plataforma de Gestión				
1. Plataforma unificada de seguridad				
1.1 La plataforma deberá ser capaz de integrarse con el sistema de Video Wall.				
1.2 Debe permitir consolidar y ejecutar todas las actividades de seguridad en una sola aplicación.				
2. Servidor				
2.1 Procesador 3.3 Ghz,8M Cache, 4C/4T turbo (80W), como mínimo.				
2.2 RAM 32 GB. DDR4-2400.				
2.3 Disco duro: 1TB 7.2 RPM SATA 6 Gbps 3.5in Cableado.				
2.4 DVD+/-RW, SATA, Interno.				

2.5 PCI Slots: 1 x Gen3 slot (x16), 2X Gen3 slot (x4), 1 x PCI				
2.6 Hasta 1 TB de almacenamiento total.				
2.7 Gigabit Ethernet LAN 10/100/1000.				
2.8 4 x USB 2.0 5 x USB 3.0, 1 x USB 3.1.				
2.9 1x DisplayPort.				
2.10 Teclado y mouse				
P. Cableado estructurado				
Todos los componentes del cableado estructurado deberán ser de categoría 6 A, todos los componentes serán de un solo fabricante, deberán cumplir con los parámetros de IEC60332-3 (se aceptará IEC60332-3C o IEC60332-33 o IEC60332-3A), LEC 60754 e IEC 61034 (se aceptará también el cumplimiento de la norma IEC 601034 en reemplazo de la norma IEC 61034), no se aceptará ningún cable de tipo CM o CMX. Como mínimo se deberá considerar los siguientes componentes: 1. Cable par trenzado categoría 6 A, deberá ser apantallado (FTP, F/UTP o U/FTP) los conductores deben ser de cobre solido calibre entre 22 a 24 AWG. 2. Modulo Jack RJ45 categoría 6 A, deberá cumplir con la norma TIA/EIA 568-C.2. 3. Patch panels con 24 Jacks RJ45 Categoría 6 A, deberá incluir 24 Jacks Categoría 6 A. 4. Patch Cords Categoría 6 A, deberá tener conectores RJ-45 a ambos extremos, se deberá suministrar un patch cords de 10 pies o de 3 mts de longitud y un patch cord de 3 pies o 1 mts de longitud, por cada punto instalado, los patch cords deberán ser instalados a través de los ordenadores horizontales, la chaqueta del patch cord deberá ser con bajo nivel de humo y libre de alógeno (LSZH) y deberá cumplir con los parámetros de 1EC60332-1. 5. Se deberá considerar como mínimo de 04 ordenadores horizontales por cada gabinete (05 gabinetes nuevos y 01 gabinete reubicado) de 88 mm x 483 x 332 mm, con cubierta trasera delantera con bisagra, el ordenador horizontal deberá ser de plástico ABS.				
R. Cámaras IP				
Aprobaciones: CE, FCC Part 15 Clase A, En la lista de UL, VCCI.				
Procesador de imágenes que genera imágenes de una resolución de hasta 1280x1024, color de 24 bits y hasta 30 fotogramas por segundo.				
Sensor de movimiento a través de cambio de pixeles.				

ANEXO B1

EQUIPAMIENTO PARA EL CENTRO DE OPERACIONES DE TI

I. Características técnicas

A. Piso Técnico

Se deberá instalar un piso técnico en la sala del centro de operaciones de TI, con las siguientes características:

13. El piso técnico deberá ser fabricado con alma de aglomerado de madera y planchas de aluminio.
14. El piso técnico debe ser para aplicaciones de Data Centers, Cuartos de Telecomunicaciones o Centros de Datos.
15. Espesor de 33 mm como mínimo.
16. Dimensiones de las baldosas 600 x 600 mm como mínimo.
17. Capacidad de carga distribuida mayor o igual a 1,800 kg/m2.
18. Debe contar con una lámina de aluminio en la cara anterior con la finalidad de crear una barrera contra el fuego y la humedad, así como reforzamiento del equipotencial eléctrico para mantener las propiedades de continuidad eléctrica del piso.
19. La altura del piso técnico debe ser de 15 cm. Cada pedestal debe estar fijado al piso con por lo menos 3 clavos de fijación de acuerdo a las recomendaciones del fabricante.
20. Color de los paneles del tipo técnico: blanco, gris claro o similar.
21. Se deberá proveer 01 chupón para levantar baldosas.
22. El piso técnico deberá ser instalado en el área del centro de operaciones de TI.

B. Sistema de Iluminación

Se deberá tener las siguientes consideraciones para el sistema de iluminación.

9. Se deberá considerar un mínimo de 15 luminarias (panel cuadrado led), que garanticen como mínimo luz con una iluminación de 500 lux en el plano vertical y 200 lux en el plano horizontal medido desde 1 m por encima del piso terminado en área del Centro de Operaciones de TI.
10. El sistema de iluminación debe ser para toda el área a intervenir del Centro de operaciones de TI.
11. Se deberá tomar en cuenta la Norma NFPA75. (Norma para la protección de equipos de cómputo electrónicos y equipos procesadores de datos), la distribución del mobiliario, equipamiento y la deficiencia de iluminación natural, para la distribución de luminarias.
12. Las luminarias se instalarán en el falso techo, se deberá considerar como mínimo 15 luminarias de 0.60 x 0.60mts.
13. No se aceptarán interruptores tipo dimmers.
14. No se reutilizarán luminarias existentes.
15. Las luminarias de la sala de operaciones de TI deben tener un interruptor de 03 golpes independiente ubicado al ingreso de la sala.
16. Se suministrará e instalará equipos automáticos de iluminación de emergencia con un nivel de 450 lux para ser activadas en ausencia del fluido eléctrico con autonomía de 2 horas. Como mínimo se deberá instalar 01 luces de emergencia, la ubicación de las luces de emergencia será dentro de la sala de operaciones de TI.

C. Control de Acceso

Se deberá instalar un sistema de control de acceso para la puerta principal al Centro de Operaciones de TI.

18. Capacidad de almacenamiento mínimo de 10,000 huellas digitales.
19. Sensor óptico: (OP5).
20. Debe manejar mínimo 32 zonas horarias.
21. Conectividad a sitios remotos por medio de red (TCP/IP). El dispositivo deberá permitir la conexión con un ordenador mediante TCP/IP, para que pueda recibir todos los datos obtenidos sin necesidad de realizar ninguna configuración en el sistema antes de poder utilizarlo. Además, puede conectarse de forma remota a su control de acceso y presencial.
22. Lector biométrico 1:1
23. Soporte de credenciales móviles, con escaneo QR o NFC.
24. Sensor de huella digital de 500 dpi/nivel de gris 256.
25. Área de detección: 23 x 23 mm.
26. Tiempo de identificación c= 1 seg.
27. Debe proporcionar un solo punto de administración, sin importar los autenticadores que se hayan definido para los usuarios
28. Taza de falsos rechazos (FRR) máxima de 0.001%.
29. Taza de falso emparejamiento (FAR) máxima de 0.0001%.
30. I/O Interface: Ethernet, RS485, RS232, Wiegand, TTL input, Relay, USB.
31. El grado de protección del sistema de control de acceso debe poseer una protección contra sedimentaciones de polvo en el interior y tenga protección contra agua nebulizada (spray), lo cual corresponde al grado de protección IP53.
32. El control de acceso debe ser monitoreable desde la red de datos y la plataforma de gestión.
33. Se debe considerar un pulsador de salida para la puerta principal.

D. Construcción en seco, sellado, pintura de paredes, pisos y puertas

15. Se deberá realizar la reubicación de la puerta de vidrio principal según plano, considerar el acondicionamiento de la pared de drywall producto de la reubicación.
16. Se deberá acondicionar la pared de drywall para la instalación de la puerta de vidrio.
17. La estructura metálica de la pared de drywall, estará conformada por perfiles de acero galvanizado, los parantes deberán ser colocados por lo menos cada 0.40 m. y deberán llevar en su interior lana de roca.
18. Las paredes deberán ser resanadas y pintadas con pintura resistente al fuego color blanco o “gris claro luz de día” para mejorar la iluminación de la sala.
19. Se deberá retirar los 03 televisores actualmente instalados y el resanamiento de la pared afectada.
20. Se deberá desmontar y retirar los gabinetes de melamine adosados a la pared, se deberá resanar la pared luego del desmontaje.
21. El Contratista deberá acondicionar las nuevas ubicaciones de los circuitos, toma eléctrica estabilizadas y comerciales, luminarias y puntos de cableado estructurado. Los cables eléctricos de las luminarias e interruptores para la sala de operaciones de TI vienen del tablero de distribución comercial del segundo piso. El Contratista deberá considerar bandeja porta cable tipo malla y/o tubería metálica EMT, para

la instalación de las nuevas luminarias e interruptores, circuitos eléctricos, control de acceso, video Wall, detección de incendio, Workstation y demás componentes a implementar.

22. El cableado estructurado, viene del cuarto de telecomunicaciones del 1er piso, a través de bandeja metálica existente hasta el falso techo, bajando a la sala de TI a través de canaleta y tubería empotrada en pared.
23. Se deberá realizar el cambio de persiana de ventana de oficina.

E. Detección de Incendios

10. El sistema de detección de incendios que se implemente deberá estar aprobado y normado por códigos nacionales e internacionales, como son:
    - 10.1 NFPA 72 National Fire Alarm Code.
    - 10.2 NFPA 70 National Electrical Code.
    - 10.3 Código Eléctrico Nacional.
11. El servicio de implementación del sistema de seguridad contra incendios deberá considerar, como mínimo, con los siguientes componentes:
    - 11.1 Panel de control para detectores inteligentes.
    - 11.2 Batería de respaldo de 07AH de capacidad.
    - 11.3 Detectores fotoeléctricos inteligentes.
    - 11.4 Anunciador audible y luminoso.
12. Detectores fotoeléctricos de humo.
13. Anunciador audible y luminoso.
14. Registro de eventos.

F. Sistema de Video Wall (4x2)

12. Deberá tener rack o soporte de montaje que permita la colocación de las pantallas a la altura mínima de 1.45 mts del piso, micro ajustable que permita una alineación precisa. Fabricado en acero de carbono, montaje con liberación rápida de pantalla que facilite el mantenimiento, con pintura electroestática.
13. Resolución de 1920 X 1080.
14. Tecnología de panel LED.
15. Tamaño mínimo de los monitores: 55 pulgadas.
16. Relación de contraste: 1000:1 contraste dinámico, como mínimo.
17. Conectividad: DVI-I (D Sub Common), Display Port 1.2 (1), HDMI 2.0 (2), stereo Mini Jack, USB 2.0 x 1.
18. Montaje tipo VESA.
19. Con Fuente de alimentación auto voltaje de 100 – 240VAC, de 50 o 60 Hz, consume típico 180 W, y un máximo de 297 W.
20. Condiciones de operación: Temperatura de 0° a 40° C, humedad relativa de 10 a 80 % sin condensación.
21. Con certificación FCC, CE, UL o equivalente.
22. Accesorios: Manuales de instalación, garantía, cable power, cable HDMI, Cable DVI, control remoto con baterías incluidas.
23. Se debe retirar los 3 monitores actualmente instalados.

G. Controlador de Video Wall

7. Procesador: 6 núcleos, 12 subprocesos, frecuencia del procesador 3,70 Ghz.
8. RAM de 16 GB.

9. Sistema Operativo compatible con la solución de Video Wall propuesta.
10. El paquete de software deberá contar con licencia de usuarios, opciones incluidas: Captura de red ilimitada, hasta 12 decodificadores IP de strems HD.
11. Se deberá considerar 01 fuente redundante y 01 disco duro redundante.
12. El controlador de video Wall, deberá generar múltiples formas de visualización. Se deberá configurar y guardar las visualizaciones y colocarlas en el video wall según se requiera.
13. El proveedor deberá instalar el servidor en un gabinete el mismo que formará parte de la mueblería del Centro de Operaciones de TI.

H. Workstation

13. Procesador de última generación, con 6 núcleos, 12 subprocesos, de 5.00 GHz Frecuencia, como mínimo.
14. RAM de 32 GB. DDR4-2400, LPDDR3-2133, como mínimo.
15. Tarjeta de video, resolución 4096 x 2160, conectores Dual conexión DVI-I y HDMI, memoria 2 G, como mínimo.
16. Sistema Operativo compatible con la solución de video Wall propuesta.
17. Placa del sistema 7x 1.2, DVI, VGA, HDMI, como mínimo.
18. Disco duro rápido y grande (SSD 512 GB), como mínimo.
19. Deberá contar con licenciamiento del sistema operativo. Así como teclado y mouse.
20. Conectividad con el controlador del Video Wall opciones incluidas: Captura de red, hasta 12 decodificadores IP de streams HD.
21. Monitor de 24 pulgadas IPS, 1920 X 1080, HDMI / DP / miniDP / USB / Audi. Brillo 250 cd/m2, contraste 1000:1, relación de aspecto 16:9, tiempo de respuesta 6ms, autovoltaje.
22. 10/100/100 Ethernet.
23. Soporte doble brazo giratorio, montaje universal, altura regulable Min. 10.0 cm. Max 42.0 cm, inclinación 30° giro lateral 360° independiente, soporte hasta 16 Kg, fabricado en aluminio.
24. Cantidades: 10 Workstation y 20 monitores como mínimo.

I. Mobiliario

1. Se deberá implementar mobiliario para el Centro de Operaciones de TI, el cual contará con lo siguiente:

   1.1 03 estaciones rectas de melamine con cajoneras movibles, como mínimo. Esto para los operadores (tener en consideración que cada Workstation va a contar con 2 monitores). Adicionalmente, se deberá instalar 03 credenzas con puertas, la credenza del centro se empleará para la instalación del equipamiento del centro de operaciones TI, las dimensiones de las credenzas deberán estarán en función al equipamiento que se instalará en la credenza del centro, además deberá garantizar el correcto funcionamiento del equipamiento instalado en él.
   1.2 07 muebles de oficina de melamine 1.20 x 0.80 x0.75 mts con cajoneras móviles.
   1.3 10 sillones ergonómicos, como mínimo.

2. Las estaciones rectas de melanine se instalarán en el Centro de Operadores de TI, en las cuales se colocarán los Workstation y monitores de 24” (se requiere dos brazos articulados por estación), que

tiene como finalidad servir de herramientas de trabajo de los operadores, estas también contarán con dos cajas para toma eléctrica y una caja toma datos. Los operadores contarán con una silla ergonómica para el confort de los operadores durante el periodo de trabajo.

3. Estaciones rectas
   3.1 Las estaciones deberán contar con base para albergar 1 Workstation.
   3.2 Medidas 1.20 x 0.66 x 0.75 metros.
   3.3 Estructura metálica electro soldado de perfil cuadrado, con acabado de pintura de aplicación electroestática.
   3.4 Tablero de melanina color blanco de 25 mm.
   3.5 Tapacantos de PVC de 03mm termo fusionados.
   3.6 Cajoneras movibles.
   3.7 04 Caja de tomas metálica, (03 troqueles) fabricado en PL LAF 1/32.
   3.8 Canaleta pasa cable.
4. Muebles de oficina
   4.1 Las estaciones deberán contar con base para albergar 1 Workstation.
   4.2 Medidas 1.20 x 0.80 x 0.75 metros.
   4.3 Estructura metálica electro soldado de perfil cuadrado, con acabado de pintura de aplicación electroestática.
   4.4 Tablero de melanina color blanco de 25 mm.
   4.5 Tapacantos de PVC de 03mm termo fusionados.
   4.6 Cajoneras movibles.
   4.7 04 Caja de tomas metálica, (03 troqueles) fabricado en PL LAF 1/32.
   4.8 Canaleta pasa cable.
5. Silloneras ergonómicos
   5.1 Araña de aluminio.
   5.2 Garruchas de Nylon PU.
   5.3 Mecanismo neumático basculante, con ajuste de tensión y regulable en reclinación.
   5.4 Brazos regulables en altura.
   5.5 Peso máximo 120-150 Kg.
6. 02 locket adosados a la pared que deberá ser construido en melamine color blanco de 25mm, con tapacantos de PVC de 03mm termo fusionado. El locket deberá tener 08 comparticiones con puerta y chapa. La distribución de los compartimientos será distribuida en dos niveles. Las medidas del locket 1.50 mts x 1.20 mts x 0.40 mts. El locket deberá estar asegurado a la pared.
7. Mesa de reuniones que permita como mínimo de 05 personas deberá incluir 04 sillas (1.20 mts).
8. Pizarra de vidrio adosable a pared.

J. Sistema Eléctrico Estabilizado y Comercial

1. El contratista será el responsable de realizar el diseño del Sistema de electricidad estabilizada y comercial.
2. El contratista deberá considerar en su diseño la reubicación y distribución de los puntos eléctricos estabilizado y comercial para la implementación del Centro de Operaciones de TI.
3. El MEF cuenta con 01 UPS de 100 KVA, los UPS se encuentra en el cuarto de comunicaciones del 1er piso Casa Grace.
4. Los interruptores termo magnéticos deberán ser automáticos, de disparo interno que permitirá la desconexión de la fase del circuito al sobrecargarse o cortocircuitarse una sola línea.

5. Todos los conductores de distribución y tomacorrientes serán de cobre con forro de material termoplástico LSHZ y se usará como mínimo el calibre de 4mm2, salvo indicación.
6. Los conductos de sección igual o superior al calibre 4mm2 serán cableados.
7. El sistema de Control de Acceso debe tener integrado batería de respaldo de mínimo 06 horas de autonomía.
8. El Contratista deberá conectar a tierra todos los equipos, canalizaciones metálicas, gabinetes, estructuras metálicas y piso técnico instalado.
9. Los equipos a instalarse, así como los accesorios necesarios deberán cumplir con las normas del Código Nacional de Electricidad y la correspondiente norma NEC 250.
10. Los conductores de protección de cobre para la puesta a tierra deben estar acorde con la NTP 370.053. En ningún caso la sección nominal del conductor de puesta a tierra podrá ser menor a 10 mm2.
11. El contratista deberá conectar a tierra todos los gabinetes y equipos dentro de ellos.
12. Se empleará tuberías metálicas del tipo EMT para la distribución. Las tuberías metálicas del tipo EMT serán elaboradas según las normas lTl NTEC-Perú. El diámetro de las tuberías EMT será recomendado por el proveedor.
13. El radio mínimo de curvatura será superior a 6 veces el diámetro exterior de la tubería, no permitiéndose en ningún caso ángulos menores de 90°.
14. Las uniones entre tuberías serán por medio de uniones de fábrica.
15. Las tuberías serán continuas entre cajas y serán colocadas en lo posible en línea recta o en su efecto con curvas suaves.
16. Las uniones de tuberías a caja se efectuaron con "conexiones a caja" del mismo material que la tubería. Todas las salidas, empalmes y conexiones de conductores eléctricos, para las derivaciones de la instalación eléctrica se harán con cajas metálicas de fierro galvanizado pesado.
17. El contratista deberá realizar la distribución del cableado eléctrico estabilizado y el cableado eléctrico comercial, para la instalación de los distintos componentes a instalarse en el Centro de Operaciones de TI.

K. Cableado estructurado

Se deberá considerar cableado estructurado para el Video Wall, estaciones de trabajo, control de acceso y demás componentes de la solución propuesta.
Se deberá considerar un punto de red categoría 6A, por cada estación de trabajo.
Todos los componentes del cableado estructurado deberán ser de categoría 6 A, todos los componentes serán de un solo fabricante, deberán cumplir con los parámetros de IEC60332-3 (se aceptará IEC60332-3C o IEC60332-33 o IEC60332-3A), LEC 60754 e IEC 61034 (se aceptará también el cumplimiento de la norma IEC 601034 en reemplazo de la norma IEC 61034), no se aceptará ningún cable de tipo CM o CMX.,
Como mínimo se deberá considerar los siguientes componentes:

1. Cable par trenzado categoría 6 A, deberá ser apantallado (FTP, F/UTP o U/FTP) los conductores deben ser de cobre solido calibre entre 22 a 24 AWG.
2. Modulo Jack RJ45 categoría 6 A, deberá cumplir con la norma TIA/EIA 568-C.2.

3. Patch panels con 24 Jacks RJ45 Categoría 6 A, deberá incluir 24 Jacks Categoría 6 A.
4. Patch Cords Categoría 6 A, deberá tener conectores RJ-45 a ambos extremos, se deberá suministrar un patch cords de 10 pies o de 3 mts de longitud y un patch cord de 3 pies o 1 mts de longitud, por cada punto instalado, los patch cords deberán ser instalados a través de los ordenadores horizontales, la chaqueta del patch cord deberá ser con bajo nivel de humo y libre de alógeno (LSZH) y deberá cumplir con los parámetros de 1EC60332-1.

Sistema de Canalización, para el sistema de canalización de datos, voz y video, se deberá considerar bandeja porta cable tipo malla galvanizada en caliente. La bandeja porta cable deberá ser fabricado con hilos de acero soldados juntos y plegados en sus formas finales.
La malla de la bandeja porta cable deberá ser de 50 mm x 250 mm como mínimo, garantizando en todo momento un 40 % de crecimiento. Las bandejas deberán ser instaladas, debajo del piso técnico, según la distribución del equipamiento propuesto (cableado estructurado, control de acceso y demás componentes de la solución propuesta).
Para el sistema de canalización del sistema eléctrico, se deberá considerar bandeja porta cable tipo malla galvanizada en caliente. La bandeja porta cable deberá ser fabricado con hilos de acero soldados juntos y plegadas en sus formas finales.
La malla de la bandeja porta cable deberá ser de 50 mm x 250 mm como mínimo, garantizando en todo momento un 40 % de crecimiento. Las bandejas deberán ser instaladas, debajo del piso técnico, según la distribución del equipamiento propuesto (cableado eléctrico a los Workstation, control de acceso y demás componentes de la solución propuesta).

Switch de 24 puertos, se deberá considerar la instalación de un switch 10/100/1000 de 24 puertos. El switch deberá contar con fuente redundante (02 fuentes de poder), los cuales podrán ser reemplazados en caliente, sin necesidad de apagar el switch. Todos los 24 puertos deberán soportar Power over Ethernet Plus (PoE+).
El switch deberá contar con 04 puertos uplinks de 10 Gb cada uno.

ANEXO B2

EQUIPAMIENTO PARA EL CENTRO DE OPERACIONES DE TI

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

a) Levantamiento de Información

30. Se debe realizar el levantamiento de información para la instalación del piso técnico, sistema eléctrico, detección de incendios, control de acceso, video Wall y mobiliarios.

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. Se debe implementar un sistema de control de acceso de tipo biométrico mediante huella dactilar, escaneo QR o NFC y credencial móvil, que incluya cerradura electromagnética.
3. Se debe retirar circuitos y tomas eléctricos y de cableado estructurado, luego se deberá nivelar y pintar las paredes de material noble y Drywall con pintura resistente al fuego color blanco o “gris-claro-luz de dia”.
4. Se deberá retirar el acabado del piso existente del centro de operaciones de TI, resanar el piso con cemento y pintar con resinas epóxicas color ladrillo, dicha pintura debe cubrir los muros perimetrales hasta la altura del piso técnico.
5. Se debe instalar un bloque de 08 pantallas y el controlador del video wall.
6. Se debe realizar una configuración especial de pantallas o monitores profesionales que se sincronizarán para mostrar contenidos, usando como interfaz un controlados y Workstation como equipos de trabajo que enviarán el contenido.
7. Se debe instalar y configurar el controlador para video Wall, el cual será Pre-cargado con el software de administración de contenido.
8. Se debe instalar y configurar el controlador del Sistema de Video Wall.
9. Se debe instalar como mínimo 10 workstation con 20 monitores de 24 pulgadas.
10. Se debe crear privilegios de seguridad avanzados y creación de Particiones: que permita definir quién tiene acceso a su sistema de seguridad física y lo que pueden hacer mediante privilegios individuales y la creación de particiones en el sistema.
11. Se debe instalar el sistema de cableado estructurado para todos los componentes ofertados, tales como; Video Wall, Workstation, Sistema de Control de acceso, Sistema de Detección de Incendios y demás componentes que lo requiera.
12. Se debe instalar y configurar un sistema de detección de incendios.
13. Se debe documentar todos los procedimientos realizados en la implementación del centro de operaciones de TI.

c) Pruebas y puesta en marcha

1. Las inspecciones y pruebas se realizarán una vez culminadas la implementación del Acondicionamiento del Centro de operaciones de TI.
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 y el MEF ejecutarán en forma conjunta los procedimientos de inspección.
4. Los procedimientos de inspección incluirán como mínimo:
    - Detalle de las actividades a realizar por el MEF, 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 el MEF o el CONTRATISTA.

5. Cualquier defecto notificado por el MEF 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 el MEF.

ANEXO B3: PRESTACIÓN ACCESORIA

EQUIPAMIENTO PARA EL CENTRO DE OPERACIONES DE TI

CONTRATACION DEL SERVICIO DE CONTINUIDAD OPERATIVA

1. Consideraciones generales

- Este servicio cubrirá todo el hardware y software ofertado.
- La prestación de este servicio es a partir del día siguiente de la conformidad de la prestación principal, y tendrá una duración 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.
- Las labores técnicas a realizar sobre la solución se llevarán a cabo en el lugar donde esta se encuentra instalada.
- 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.
- 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, por vía telefónica o por mensajería instantánea. 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 atendido 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.

2.1.2. Soporte técnico

- El Servicio de Soporte Técnico debe brindarse en modalidad 24x7x365, incluyendo fines de semana y feriados.
- 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. En caso de falla, inoperatividad o problema el contratista se encargará de corregir el mal funcionamiento o el riesgo tecnológico en los sistemas propuestos (Plataforma de Gestión, Video Wall, control de acceso, Equipos de Aire Acondicionado, Detección de Incendios, Sistema Eléctrico). De ser necesario, debe gestionar con el fabricante incidentes, fallas problemas o requerimientos presentados según el nivel de complejidad.
- 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 a los sistemas instalados 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.

2.2. Características y actividades del servicio de mantenimiento preventivo

- El mantenimiento preventivo se realizará sobre los bienes adquiridos, incluyen 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 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. 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 del equipamiento instalado.
- Debe ser brindada dentro de los primeros noventa (90) días calendario del servicio, contabilizado a partir del día siguiente de la conformidad de la prestación principal.
- Debe estar enfocada en las funcionalidades a nivel de administración, soporte y monitoreo de la solución instalada.
- Debe estar dirigida para siete (07) personas pertenecientes a la

OGTI. Cada una de las personas debe recibir una capacitación mínima de doce (12) horas.
- La frecuencia debe ser mínimo tres (03) veces a la semana, de lunes a viernes (fuera del horario de oficina) y sábados.

2.3.1. 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.

2.3.2. 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, 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.

2.4. 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.

2.4.1. 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 y presentación de los entregables mensuales.

2.4.2. Servicio de Mantenimiento Preventivo:

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

- Informe del 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.
  -

2.4.3. Servicio de Capacitación

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 capacitación, según detalle:

- Documento de Capacitación.
  - Nombre del personal
  - Temario
  - Cantidad de horas de la capacitación brindada.
  - Certificados de los participantes de la capacitación.

3. Nivel de Servicio

Se requiere un soporte técnico ante fallas o problemas con la solución propuesta (Sistema de Iluminación, Control de Acceso, Detección de Incendio, Sistema de Video Wall, Controlador de Video Wall, Workstation, Sistema Eléctrico Estabilizado y Comercial). El contratista deberá entregar su procedimiento de atención cumpliendo con lo siguiente:

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

Tipo de	Nivel	SLA (Tiempo de	Observaciones

Solicitud		atención – horas hábiles)	
Incidencias Corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo en la solución	**Alto**	**Tiempo de respuesta:** 30 minutos **Tiempo de solución:** 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.
	Medio	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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.
	Bajo	**Tiempo de respuesta:** 1 hora **Tiempo de solución:** 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 o incidentes presentados en producción sobre la solución que no afecten a usuarios, pero reducen la calidad de servicio de la solución.

TABLA N° 01: Servicio de Soporte Técnico de Incidencias

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

Tipo de Solicitud	Nivel	SLA (Tiempo de atención – horas hábiles)	Observaciones
Requerimiento Corresponde a cualquier pedido de cambio o modificación en la configuración actual.	**Medio**	**Tiempo de Respuesta** 2 horas **Tiempo de Solución** 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 soluciona 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.

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 I 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 implementados. 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.

Personal de capacitación: Será la persona encargada de brindar la capacitación en el manejo de la solución ofertada al personal designado por la OIT.
El personal para la capacitación debe estar avalado por la marca para brindar la capacitación oficial.

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 requerimientos 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	Incumplimiento De Programa O Ejecución De Trabajo. Cuando se detecte que EL CONTRATISTA incumplió el cronograma de trabajo aprobado (actividades a realizar según el plan de trabajo). Por incumplimiento total o parcial de las actividades programadas, la cual será aplicada por actividad o trabajo.	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
2	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 del servicio (por cada vez detectado).	10% UIT vigente por cada ocurrencia	Informe del área usuaria.
3	Por Incumplir con el reglamento interno de seguridad y salud en el trabajo de la prestación La penalidad será establecida 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 sanción hasta cuando ella sea subsanada.	10% UIT vigente por cada ocurrencia y por cada día de demora en subsanar	Informe del área usuaria.
4	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
5	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:

THM = 24 x 90 = 2,160 horas

THE = 4+3 = 7 horas

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%

Rango de UPTIME	Penalidad(1)
>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 el Centro de Operaciones de TI del segundo piso del edificio Casa Grace.

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

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.

9.2. 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, se realizará en doce (12) pagos trimestrales en partes iguales, luego de emitida la conformidad previa presentación de cada informe trimestral.
- Para el Servicio de Capacitación, se realizará un solo pago, luego de emitida la conformidad, previa presentación del Documento de Capacitación.

- Para el Servicio de Mantenimiento Preventivo, se realizará en seis (6) pagos en partes iguales, luego de emitida la conformidad previa presentación del informe por la realización del servicio.

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 perdida 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.
El SCTR deberá ser presentado para el inicio de la prestación y deberá estar vigente durante la ejecución del servicio.

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 Secretaria 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 dictadas por los sectores y autoridades competentes, así como las que se dicten durante el periodo de prestación del servicio.

La adecuación e 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° 972-2020-MINSA,** aprueba el Documento Técnico: "Lineamientos 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° 972-2020-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 nitrito, 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 serologías 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

24.1. 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

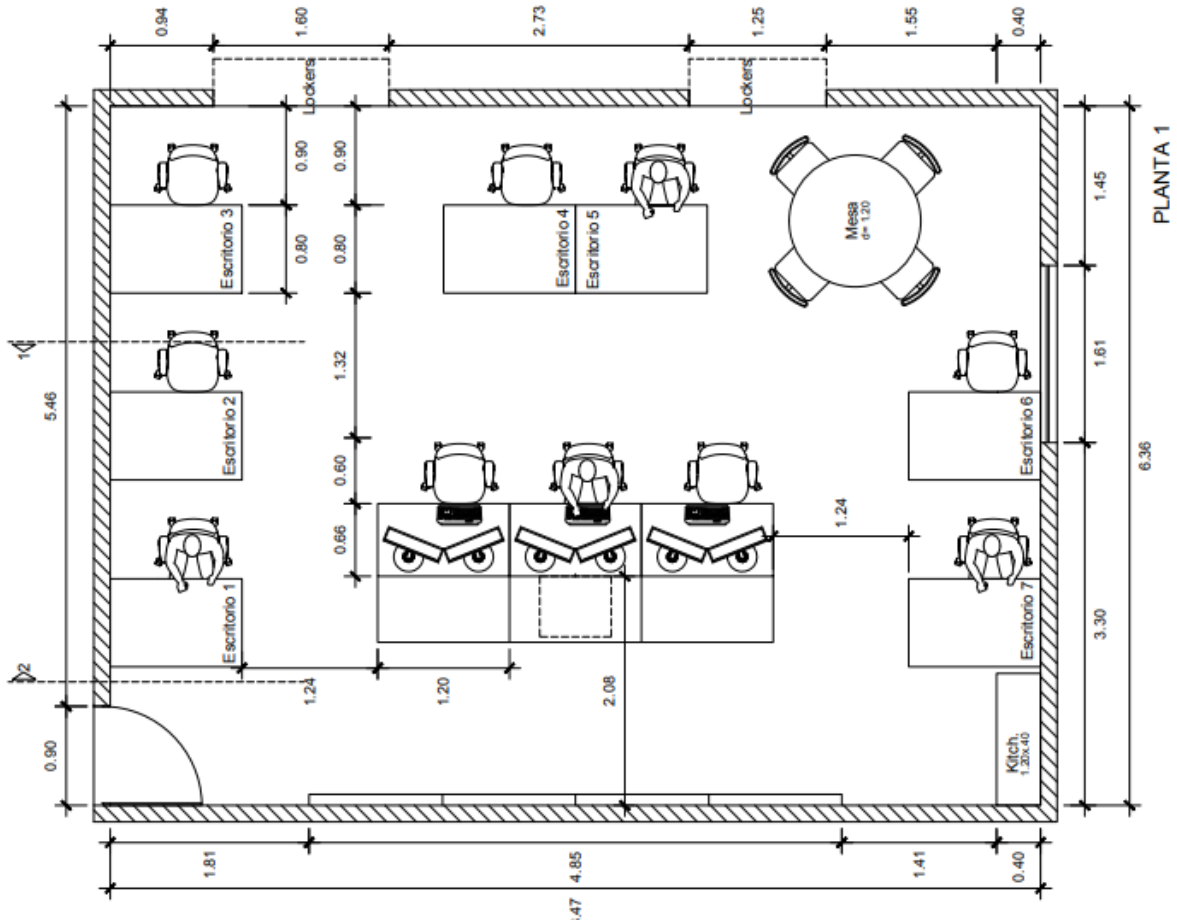
Como parte del servicio, el contratista pudiera tomar conocimiento de la información de la plataforma tecnológica y de los sistemas de información del MEF. Si este fuera el caso, esta información es reservada, por lo tanto, el contratista y todo su personal deberá mantener la confidencialidad de la misma. 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.

ANEXO B4

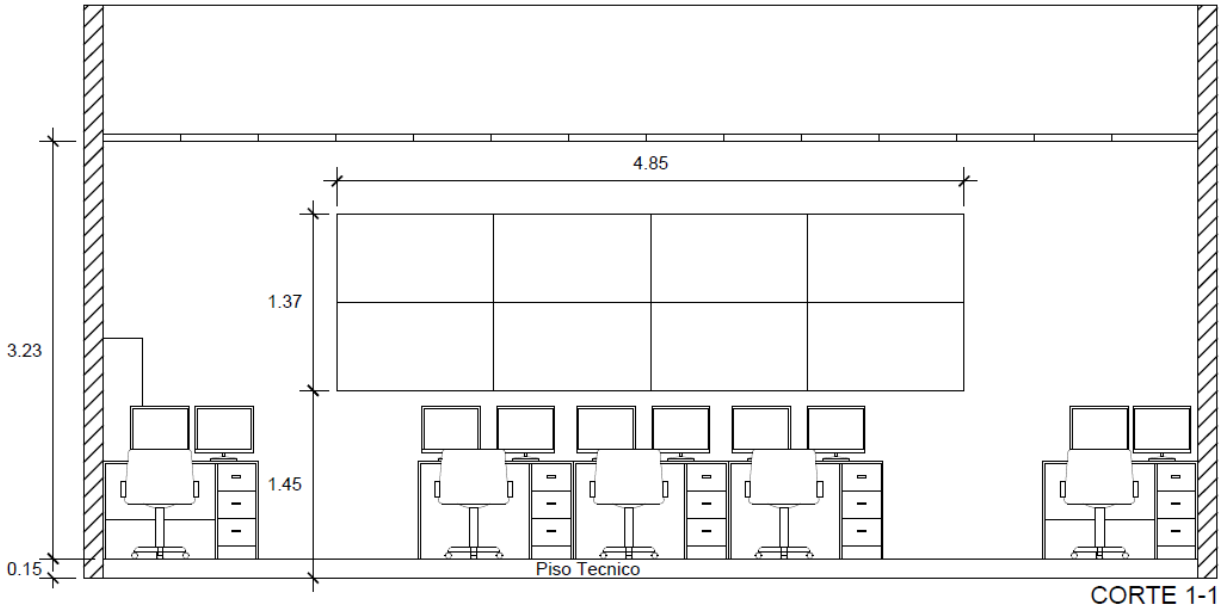
EQUIPAMIENTO PARA EL CENTRO DE OPERACIONES DE TI

Se adjuntan planos de la ubicación donde se implementará el Centro de Operaciones de TI del MEF.

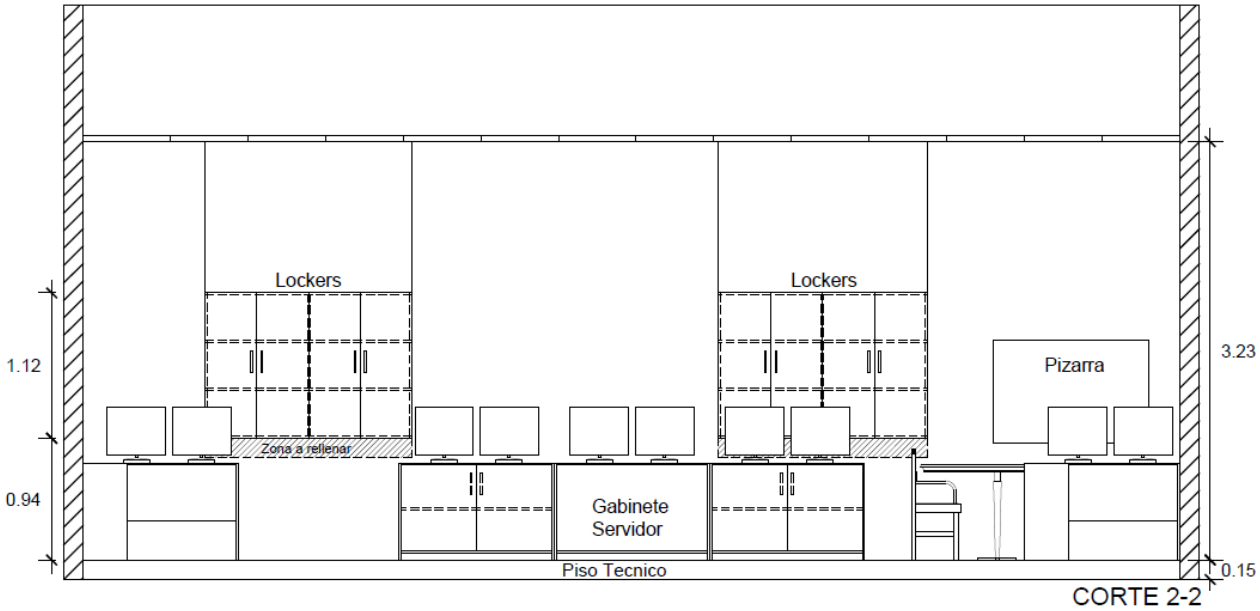
Lamina 01: Plano de distribución del Centro de Operaciones de TI del MEF



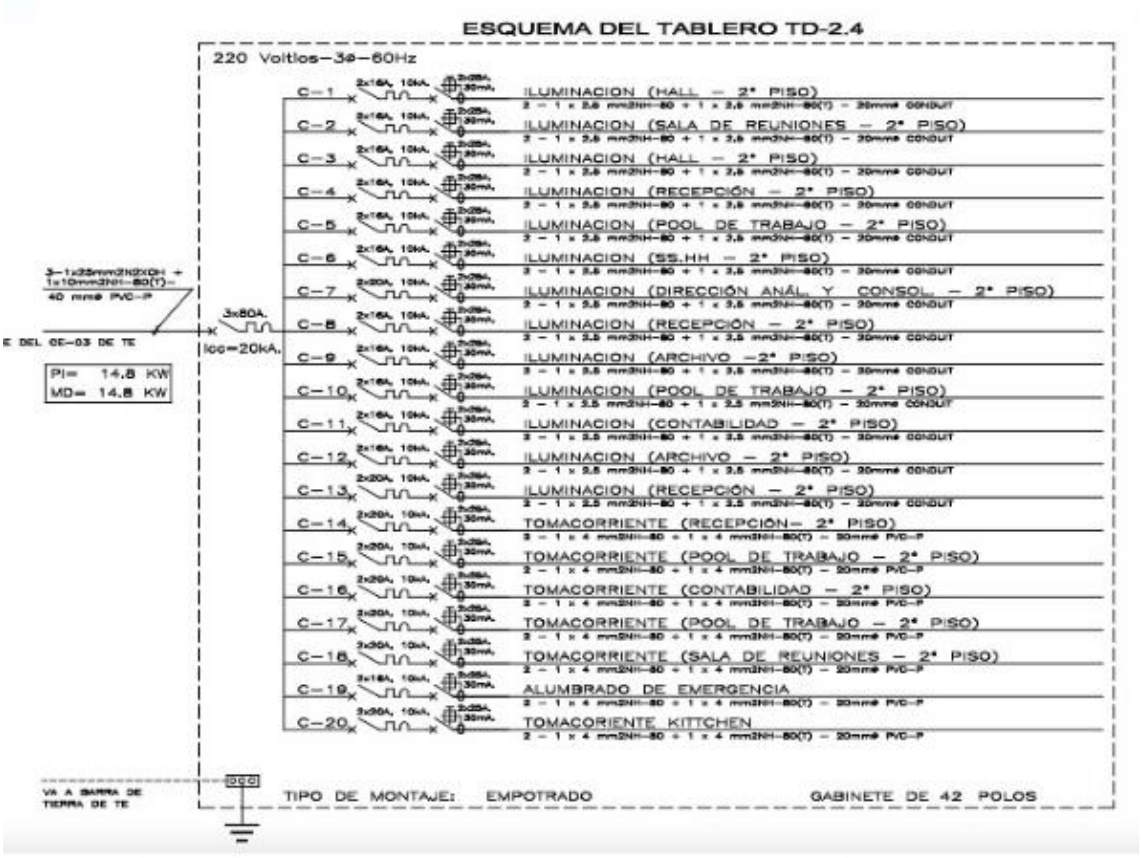
Lamina 02: Plano del Centro de Operaciones de TI del MEF – Corte 1-1



Lamina 03: Plano del Centro de Operaciones de TI del MEF – Corte 2-2



Lamina 04: Plano de diagrama unifilar del tablero comercial



ANEXO B5

Equipamiento para el Centro de Operaciones 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.**
Equipamiento para el Centro de Operaciones de TI				
A. Piso Técnico				
1. Capacidad de carga distribuida mayor o igual a 1,800 kg/m2.				
C. Control de Acceso				
1. Soporte de credenciales móviles, con escaneo QR o NFC.				
F. Sistema de Video Wall (4x2)				
1. Resolución de 1920 X 1080.				
2. Tecnología de panel LED.				
3. Relación de contraste: 1000:1, contraste dinámico.				
4. Conectividad: DVI-I (D Sub Common), Display Port 1.2 (1), HDMI 2.0 (2), stereo Mini Jack, USB 2.0 x 1.				
5. Montaje tipo VESA.				
6. Con Fuente de alimentación auto voltaje de 100 – 240VAC, de 50 o 60 Hz, consume típico 180 W, y un máximo de 297 W.				
7. Condiciones de operación: Temperatura de 0° a 40° C, humedad relativa de 10 a 80 % sin condensación.				
8. Con certificación FCC, CE, UL o equivalente.				
G. Controlador de Video Wall				

1. Procesador: 6 núcleos, 12 subprocesos, frecuencia del procesador 3,70 Ghz.				
2. RAM de 16 GB.				
3. Sistema Operativo compatible con la solución de Video Wall propuesta.				
4. Se deberá considerar 01 fuente redundante y 01 disco duro redundante				
H. Workstation				
1. Procesador de última generación, con 6 núcleos, 12 subprocesos, de 5.00 GHz Frecuencia, como mínimo.				
2. RAM de 32 GB. DDR4-2400, LPDDR3-2133, como mínimo.				
3. Tarjeta de video, resolución 4096 x 2160, conectores Dual conexión DVI-I y HDMI, memoria 2 G, como mínimo.				
4. Sistema Operativo compatible con la solución de video Wall propuesta.				
K. Cableado estructurado				
Todos los componentes del cableado estructurado deberán ser de categoría 6 A, todos los componentes serán de un solo fabricante, deberán cumplir con los parámetros de IEC60332-3 (se aceptará IEC60332-3C o IEC60332-33 o IEC60332-3A), LEC 60754 e IEC 61034 (se aceptará también el cumplimiento de la norma IEC 601034 en reemplazo de la norma IEC 61034), no se aceptará ningún cable de tipo CM o CMX. Como mínimo se deberá considerar los siguientes componentes: 1. Cable par trenzado categoría 6 A, deberá ser apantallado (FTP, F/UTP o U/FTP) los conductores deben ser de cobre solido calibre entre 22 a 24 AWG. 2. Modulo Jack RJ45 categoría 6 A, deberá cumplir con la norma TIA/EIA 568-C.2. 3. Patch panels con 24 Jacks RJ45 Categoría 6 A, deberá incluir 24 Jacks Categoría 6 A. 4. Patch Cords Categoría 6 A, deberá tener conectores RJ-45 a ambos extremos, se deberá suministrar un patch cords de 10 pies o de 3 mts de longitud y un patch cord de 3 pies o 1 mts de longitud, por cada punto instalado, los patch cords deberán ser instalados a través de los ordenadores horizontales, la chaqueta del patch cord deberá ser con bajo nivel de humo y libre de alógeno (LSZH) y deberá cumplir con los parámetros de 1EC60332-1.				