REQUERIMIENTO

1. DATOS GENERALES:

1.1 ÓRGANO Y/O UNIDAD ORGANICA

Oficina de Tecnologías de la Información.

1.2 ACTIVIDAD DEL POI / ACCIÓN ESTRATEGICA PEI

- Actividad POI: OE6. Asegurar eficiencia de la organización a través de la implementación del modelo de transformación digital.

- Acción Estratégica PEI: AEI21 Implementar el equipo, infraestructura y portafolio de proyectos de digitalización (Modelos de Gobierno Digital).

1.3 DENOMINACIÓN DE LA CONTRATACIÓN

ADQUISICIÓN Y GESTIÓN DE LICENCIAS DE ANTIVIRUS, DETECCIÓN Y RESPUESTA DE PUNTOS FINALES (EDR).

2. CLAUSULAS DE ANEXO:

2.1 FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Fortalecer la seguridad digital de propiedad de Fondo Mivivienda S.A. (FMV), alojada y gestionada en la red interna institucional, garantizando su confidencialidad, integridad y disponibilidad, mediante la implementación de controles de seguridad en los equipos finales y servidores de la entidad que permitan aplicar y supervisar políticas de seguridad a las actividades de los usuarios, evaluar y gestionar riesgos, así como detectar, contener y neutralizar malware y otras amenazas, reduciendo la probabilidad de incidentes y asegurando la continuidad operativa.

2.2 OBJETIVO DE LA CONTRATACIÓN

Contar con una solución de protección de endpoints y servidores que integre antivirus, capacidades EDR y control de puertos USB, a fin de prevenir, detectar y responder oportunamente ante amenazas, aplicando políticas de seguridad institucionales y reduciendo el riesgo sobre la información y activos digitales del FMV.

2.3 CARACTERISTICAS TÉCNICAS

La adquisición de Licencias de Antivirus, Detección y Respuesta de Puntos Finales (EDR) deberá entregarse en el plazo de un (1) día calendario e instalarse en el plazo máximo de hasta cinco (5) días calendario. Asimismo, se ha previsto una ejecución de servicio en un plazo máximo de doscientos cuarenta (240) días calendario, equivalente al periodo de ocho (08) meses, y deberá cumplir con las siguientes características técnicas mínimas:

Descripción	Equipos	Cantidad	Plazo de ejecución
Adquisición de Licencias de Antivirus, Detección y Respuesta de Puntos Finales (EDR)	Endpoints	337	240 días calendarios (equivalente a 8 meses)
	Servidores	13	

a) Descripción de funcionalidades y capacidades:

El presente servicio debe contemplar, como mínimo lo siguiente:

Fondo Mivivienda

Firmado digitalmente por ESPINOZA VILLOGAS Edgar Renan FAU 20414671773 soft
Motivo: Doy V° B°
Fecha: 03.02.2026 16:49:04 -05:00

Fondo Mivivienda

Firmado digitalmente por GUEVARA CANALES Milton Edua FAU 20414671773 soft
Motivo: Doy V° B°
Fecha: 03.02.2026 16:13:22 -05:00

- La solución deberá permitir el monitoreo y el control de dispositivos extraíbles en los dispositivos de los usuarios, como dispositivos USB y lectoras CD/DVD.
- La solución debe tener un sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints y servidores con información detallada del malware en sí y el origen de la infección.
- La solución debe poder aislar una maquina comprometida de la red de forma automática mientras la investigación del incidente.
- La solución debe poder generar un Snapshot forense (recolección de metadata asociada a la amenaza) durante una investigación de una amenaza.
- La solución debe de poder almacenar los datos de los Indicadores de Compromiso (IoC) detectados por la solución en la consola de gestión basada en nube.
- La solución debe ser capaz de contar con un reporte que diga el tiempo que los dispositivos no han tenido actualizaciones de seguridad.
- Permitir la planificación de fecha y hora para el despliegue de parches y actualizaciones, discriminando endpoints y servidores.

b) Protección contra Malware:

- La solución debe permitir la detección del malware en preejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
- La solución debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables.
- La solución debe poseer la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
- La solución debe permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
- La solución debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.

c) Control de dispositivos

- Para la protección contra el malware en dispositivos externos, la solución debe incluir un sistema de control de dispositivos que detecta el uso de dispositivos USB, grabadores de CD/DVD, lectores de CD/DVD, etc.
- El sistema debe permitir el control de dispositivos externos para permitir, bloquear y alertar.
- El sistema de control de dispositivos estará integrado en la misma consola, es decir, no requiere la instalación de programas adicionales en los equipos.

d) Protección contra Ransonware

- La solución debe disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.
- La solución debe disponer de capacidad de remediación de la acción de cifrado malicioso de ransomware tanto en ejecución local como de forma remota.
- La solución debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware o realizar un rollback a las acciones maliciosas al detectar un ransomware.
- La solución debe contar con protección Anti-Ransonware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas. Esta capacidad Anti-Ransonware debe permitir la definición granular de las carpetas a proteger en los servidores.

e) Detección proactiva de reconocimiento de nuevas amenazas

- La solución debe tener la capacidad de protección de amenazas de día cero.

- La solución debe tener funcionalidad de detección de amenazas desconocidas.
- La solución debe tener la capacidad de detección, y bloqueo proactivo de malware no conocido (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- La solución debe detectar el malware en pre-ejecución.
- La solución debe tener la capacidad de bloqueo y protección contra amenazas desconocidas potencialmente sospechosa.
- La solución debe tener la capacidad de generación de excepciones ante falsos positivos.

f) Actualización de firma y nuevas versiones de producto

- Las actualizaciones se realizarán automáticamente (programadas) y manualmente del fichero de firmas de virus y del motor de escaneado del malware en las estaciones de trabajo desde internet.
- La actualización de nuevas versiones del producto se puede realizar automáticamente y no requiere la desinstalación y/o reinstalación de algún componente previo.

g) Consola de administración en la nube

- La solución deberá contar con una consola de administración en la nube.
- La herramienta deberá permitir la administración centralizada y distribuida todas las licencias distribuidas en los endpoints y servidores.
- La consola debe sincronizarse con el Directorio Activo de FMV para la instalación automática de la solución de seguridad en los equipos. Para esto se proporcionará una máquina virtual.
- Cualquier cambio en las políticas deberán desplegarse automáticamente a los equipos sean estos Windows.
- Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad.
- El administrador deberá poder crear políticas desde la consola.
- La consola debe permitir obtener una visibilidad clara de todos sus usuarios, sus dispositivos y su estado de protección.
- La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico.
- La consola deberá almacenar un histórico de eventos de cada equipo administrado.
- El sistema para la delegación de roles deberá contener un administrador de permisos, pudiendo crear distintos perfiles con permisos particulares para cada administrador.
- La consola debe permitir visualizar por medio de dashboard los eventos, las versiones, equipos con el producto, etc.

h) Alertas y reportes

- La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alerta de registros, etc.).
- La solución deberá contener un sistema de reportes que permitir ver el estado de la protección de la red en línea. Este sistema debe mostrar en tiempo real lo que está ocurriendo en la red.

i) Sistemas operativos.

El servicio a contratar debe soportar:

- Microsoft Windows 10.
- Microsoft Windows 11.
- Microsoft Windows Server 2016, 2019, 2022.

2.3.1 CARACTERISTICAS Y CONDICIONES DE LA PRESTACIÓN

A. Desarrollo del Servicio

- Se deberá tener una reunión de Kick Off presentando el plan de trabajo, de manera virtual o presencial, según las indicaciones de la OTI, hasta los 2 días calendarios contabilizados a partir del día siguiente de notificada la orden de compra, el mismo que será coordinado previamente con el área usuaria.
- La OTI aprobará el plan de trabajo hasta 01 día calendario contabilizado a partir del día siguiente de realizar de Kick Off presentando del plan de trabajo.
- La implementación se realizará hasta los 04 días calendarios contabilizados a partir del día siguiente de aprobado el plan de trabajo.
- El contratista deberá realizar la transferencia de conocimiento de manera virtual, como mínima de 04 horas para equipo de Seguridad, presentando material didáctico. La fecha y hora, será coordinado previamente por la OTI.

		Días						
N°	Actividades	1	2	3	4	5	6	7
1	Reunión de Kick Off							
2	Aprobación del plan de trabajo							
3	Implementación y configuración							

B. Instalación e Implementación

- El contratista deberá realizar el despliegue del agente en estaciones de trabajo y servidores, de forma remota y centralizada.
- Deberá configurarse, como mínimo:
  - Políticas base de antimalware/EDR.
  - Políticas de control de dispositivos removibles (USB y otros).
  - Políticas de protección contra ransomware.
  - Alertas y reportes operativos.
- El servicio deberá incluir pruebas de funcionamiento (validación de detección, aislamiento, alertas, reportes, actualizaciones y consultas).

C. Operación y administración

- La solución deberá permitir la gestión centralizada desde la consola en la nube, incluyendo:
  - Administración de políticas.
  - Delegación de roles.
  - Estado de protección.
  - Visualización de incidentes y priorización de eventos.
- Los encargados de la OTI de FMV contarán con el perfil administrador y perfiles adicionales según necesidad.

D. Soporte y mantenimiento

- El contratista brindará soporte técnico durante la vigencia del servicio bajo un esquema de mesa de ayuda (remoto).
- Deberá incluirse atención de incidencias asociadas a:
  - Fallas del agente, despliegue y actualización.
  - Detecciones, contención y remediación.
  - Problemas de comunicación consola-agentes.
- Ajustes de políticas y excepciones por falsos positivos.

E. Transferencia de Conocimiento

- El contratista deberá realizar la transferencia de conocimiento al equipo de la OTI designado por la entidad, con la finalidad de garantizar la correcta operación, administración y continuidad del servicio. Dicha transferencia tendrá una duración mínima de cuatro (4) horas y deberá contemplar, como mínimo, los siguientes temas:

  - Administración de consola y políticas.
  - Gestión de alertas e incidentes EDR.
  - Control de dispositivos y manejo de excepciones.
  - Se entregará material (manuales).
  - Agregar indicadores de compromiso (IoC).

F. Reportes

El Contratista deberá remitir los reportes operativos o informes u otra información adicional a la OTI, mediante correo electrónico, el cual será proporcionado al momento efectivo del servicio y contabilizado a partir del día siguiente de solicitado por el área usuaria.

Servicio	Documento
Soporte técnico	Informe técnico
Copias de respaldo	
Actualizaciones y mejoras	
Respuesta a incidente	Informe de incidente

G. Requerimientos de conectividad

El servicio tendrá acceso remoto a la plataforma a ser gestionada ya sea a través de un acceso de administración remoto.

i) Niveles de servicio:

Acuerdo de Nivel de Servicio		
Servicio	**SLA**	**Entregables**
Gestor del servicio	Supervisión cotidiana.	
	Operación cotidiana a cargo del Gestor del Servicio en horario de oficina (8x5)	Informe de actividad técnica semanal. Informe de servicio mensual.
Cambios, configuraciones y maniobras	Número de solicitudes: Ilimitado Horario: 8x5 (SLA: P2, P3 o P4)	Solicitud/resolución individual.
Respuesta a incidente	Número de solicitudes: Ilimitado Horario: 8x5 (SLA: P1, P2, P3 o P4)	
Soporte técnico	Número de solicitudes: Ilimitado Horario: 8x5 (SLA: P1, P2, P3 o P4)	

Copias de respaldo	Periodicidad: Semanal (SLA: 99.8% de cumplimiento)	Informe técnico
Actualizaciones y mejoras	Periodicidad: De acuerdo con el plan de mejoras. SLA:99.8% de cumplimiento.	
Servicio de Gestión de vulnerabilidades.	Periodicidad: Trimestral	

Acuerdos de Nivel de Servicio				
Tiempos de Atención para Cambios, Configuraciones, Maniobras y Soporte				
P5	P4	P3	P2	P1
Nivel de Informacional	Nivel bajo o rutina	Nivel medio/moderado	Nivel alto	Nivel crítico o de emergencia
Tiempos de Ejecución para Cambios y Configuraciones (en el 90% de los casos)				
48 horas	24 horas	12 horas	6 horas	3 horas
Tiempo de Resolución Esperada para incidentes				
24 horas	8 horas	4 horas	3 horas	2 horas
Correo/ Asistencia remota				
24 horas	5 horas	2 horas	1 hora	30 min.
Los tiempos SLA se contabilizan en horas desde el ingreso de la solicitud.				
Algunas labores de cambios y configuraciones complejas requieren acciones de planificación, validación o pruebas complementarias y que incluso pueden depender de proveedores terceros.				

ii) Niveles de Criticidad para Incidencias

Nivel	Situación	Prioridad
Crítico o de emergencia	Afecta la operatividad total de la organización, que requiere una asistencia remota.	P1
Alto	Afecta la operatividad total de los servicios no críticos de la organización y que probablemente afecte los sistemas críticos de la organización en el corto plazo.	P2
Medio o moderado	Para reportar algún incidente respecto a la afectación parcial de un equipo o exista impacto a un servicio de la organización.	P3
Bajo o rutina	Para realizar consultas o reportar algún incidente que no afecte la operación del equipo.	P4
Informacional	Se incluyen también actividades de intercambio de información donde no se requiere ninguna acción	P5

i) Canales de atención:

- Telefónico: Se brindará a través de medios de telefonía fija o móvil.
- E-mail y Chat: Se brindará a través de comunicación electrónica como e-mail y chat (mensajería instantánea). Para el caso de e mail, se recibirán nuestras consultas o solicitudes de soporte en la dirección de correo que se establezca.
- Atención Remota (control remoto): Se ejecutará mediante procedimientos especiales de conexión remota, el cual es un método rápido y seguro.

2.3.2 ALCANCES DEL SERVICIO

El servicio tiene por finalidad implementar un servicio de protección para endpoints y servidores que integre capacidades de antivirus, EDR y control de dispositivos removibles, a fin de prevenir, detectar, contener y responder oportunamente ante amenazas, aplicando políticas de seguridad y generando registros y reportes para la trazabilidad y gestión de incidentes.

2.3.2.1 Alcance técnico

El servicio deberá comprender como mínimo las siguientes actividades:

- Implementación y despliegue de agente
  - Instalación y configuración del agente de seguridad en estaciones de trabajo Windows 10/11 y servidores Windows Server 2016/2019/2022.
  - Verificación de conectividad con la consola, estado de salud del agente, actualización de firmas y aplicación inicial de políticas.
  - Para el despliegue del agente en los puntos finales (endpoints y servidores), se requiere que este se realice inicialmente de manera masiva, mediante una GPO u otro mecanismo que permita su instalación sin generar interrupciones al usuario.

- Configuración de políticas de protección
  - Activación y ajuste de capacidades EDR para detección, investigación y respuesta, incluyendo priorización de alertas e incidentes.

- Control de dispositivos
  - Definición e implementación de políticas para permitir, bloquear y alertar el uso de dispositivos removibles (USB y otros) por perfiles de usuario, grupo y/o equipo.

- Operación de seguridad y respuesta a incidentes
  - Configuración de acciones de contención y remediación y aislamiento del equipo cuando corresponda.

- Alerta, reportes y trazabilidad
  - Configuración de notificaciones y reportes operativos.
  - Consolidación de dashboards e indicadores mínimos.

2.3.2.2 Duración del servicio

Deberá ejecutarse en un plazo máximo de ocho (08) meses calendario, contados a partir del día siguiente de instalado el Software.

2.3.2.3 Certificaciones del proveedor

- Contar con certificado ISO 27001:2022 con enfoque a los procesos o servicios de ciberseguridad.

Asimismo, para la acreditación de ello, deberá presentar copia simple del certificado correspondiente.

2.4 REGLAMENTOS TÉCNICOS, NORMAS METRÓLOGICAS Y/O SANITARIAS

No aplica al presente requerimiento.

2.5 ACONDICIONAMIENTO, MONTAJE E INSTALACIÓN

No aplica al presente requerimiento.

2.6 GARANTÍA COMERCIAL

No se requiere garantía comercial.

2.7 MUESTRAS

No aplica al presente requerimiento.

2.8 PRESTACIONES ACCESORIAS

No se ejecutan prestaciones accesorias.

2.9 REQUISITOS DEL PROVEEDOR

2.9.1 REQUISITOS OBLIGATORIOS

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/100,000.00 (quinientos mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez (10) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 20,000.00 (quinientos mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran bienes iguales o similares a los siguientes: Venta o Adquisición y Gestión de licencias de Antivirus.

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 constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o la cancelación del mismo con comprobante de pago, o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

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 7** referido a la Experiencia del Postor en la Especialidad.

En el caso de suministros de bienes, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (08) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

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

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo8**.

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad que le hubiesen transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo 7** referido a la Experiencia del Postor en la Especialidad.

B. CAPACIDAD TÉCNICA Y PROFESIONAL

B.1 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

Un (1) Gestor de Proyecto:

Experiencia mínima de tres (03) años como Gestor o Coordinador o Supervisor de proyectos en ciberseguridad o Seguridad de la Información o Seguridad informática o soluciones de antivirus.

Acreditación:

La experiencia del personal clave se acredita 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.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.

Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas.

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

En ningún caso corresponde exigir al personal que cumpla con experiencia en más de un cargo de forma simultánea.

B.2 CALIFICACIONES DEL PERSONAL CLAVE

B.2.1 FORMACIÓN ACADÉMICA

Requisitos:

Un (1) Gestor de Proyecto:

Titulado o Bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas y Computo o Ingeniería de Computación y Sistemas o Ingeniería de Sistemas e Informática o Ingeniería de Computación o Ingeniería Informática y/o de Sistemas o Ingeniería de Sistemas Empresariales o Ingeniería Industrial o Ingeniería de Sistemas de Información o Ingeniería de Telecomunicaciones o Ingeniería de Redes y Comunicaciones de Datos.

Acreditación:

El Grado de Título o Bachiller es verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda.

El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso el Grado de Bachiller no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

B.2.2 CERTIFICACIONES

Requisitos:

Un (1) Gestor de Proyecto:

Certificado PMP vigente emitido por el PMI.

Acreditación:

La experiencia del personal clave se acredita 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.

2.10 PLAZO DE EJECUCIÓN:

- Plazo de entrega e instalación:

  La adquisición de Licencias de Antivirus, Detección y Respuesta de Puntos Finales (EDR) deberá entregarse en el plazo de un (1) día calendario contado desde el día siguiente de la notificación de la orden de compra.

  Asimismo, dicho software deberá instalarse en el plazo máximo de hasta cinco (5) días calendario, contados a partir del día siguiente de su entrega.

- Plazo de ejecución del servicio:

  El plazo de ejecución del servicio se realizará en un plazo máximo de 240 días calendarios, equivalente a ocho (08) meses, contabilizados a partir del día siguiente de suscrito el contrato y/o notificada la orden de servicio, según corresponda.

2.11 ENTREGABLES

Los entregables, que corresponden a la etapa del servicio, deberán ser presentados en formato digital, teniendo en cuenta los plazos indicados a través de los siguientes medios:

- Mesa de partes presencial, ubicado en el primer piso de Calle Amador Merino Reyna 281 – San Isidro, en el Horario de 08:30 a 17:30 horas.

- Plataforma de Mesa de partes virtual, la misma que tiene condiciones de uso en el siguiente enlace: https://www.mivivienda.com.pe/smpv/#/formulario.

1. La entrega del certificado o evidencia del registro del servicio en el sitio web o documento equivalente que acredite el derecho del FMV de recibir el aseguramiento de software por el plazo contratado, a más tardar hasta los cinco (05) días calendarios, contabilizados a partir del día siguiente de haberse suscrito el contrato el mismo que será coordinado previamente con el área usuaria.
2. El proveedor deberá presentar el plan de trabajo en una reunión de Kick Off.
3. Hasta los cinco (05) días calendarios de culminado el mes anterior se deberá presentar de manera mensual lo siguiente:
   - Informe resumen del soporte técnico, copias de respaldo, actualizaciones o mejoras, respuestas a incidentes durante el mes transcurrido u Operaciones (atenciones a requerimientos) en el período.
   - Informe técnico mensual del del estado de salud de la consola.
   - Informe ejecutivo del servicio de acuerdo con el periodo ejecutado.
4. Hasta los cinco (05) días calendarios de culminado el trimestre anterior deberá presentar de lo siguiente:
   - Resultados del escaneo de vulnerabilidades.
   - Informe ejecutivo del escaneo de las vulnerabilidades.

2.12 CONFORMIDAD

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas. La conformidad será otorgada por el Jefe de la Oficina de Tecnologías de la Información, en el plazo máximo de siete (07) días computados desde el día siguiente de producida la recepción.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para

subsanar el cual no debe ser mayor al 30% del plazo de la entrega del bien y del entregable[1] correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

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

2.13 FORMA Y CONDICIONES DE PAGO

a. Modalidad de pago

El contrato se rige por la modalidad de **SUMA ALZADA**, de conformidad con el artículo 130 del Reglamento.

b. Adelantos

No aplica el pago de adelantos para la presente contratación.

c. Forma de pago:

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA en **SOLES**, en **PAGOS PARCIALES** *posterior a la entrega e instalación de los bienes, y posteriormente, luego de la presentación de cada entregable mensual según el numeral 2.11*., luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

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

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de Oficina de Tecnología de la Información (OTI), previo visto bueno del Supervisor de seguridad y proyectos de TI. (Proporcionado por la Entidad)
-
- Comprobante de pago (XML y PDF).
- Orden de compra (Proporcionado por la Entidad).
- Consulta de Autorización de Comprobantes de pago (ingresando a la página web de la SUNAT por la entidad).

Dicha documentación se debe presentar por el contratista a través del canal de Mesa de partes virtual: https://www.mivivienda.com.pe/sgd.mpv/

El comprobante de pago deberá indicar el número de contrato, el número de la orden de servicio o contrato y emitida a nombre de:

- Razón Social: FONDO MIVIVIENDA S.A.

[1] En caso de que el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad contratante efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto.

- Dirección: Cal. Amador Merino Reyna N°285 – Edificio Targa-San Isidro
- RUC:20414671773
- Teléfono:211-7373

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (07) días del día siguiente de recibido el bien, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

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

En caso de retraso en el pago por parte de LA ENTIDAD CONTRATANTE, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la N°32069, Ley General de Contrataciones Pública.

2.14 RESPONSABILIDAD DEL PROVEEDOR

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

2.15 PENALIDAD POR MORA

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40

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

Las penalidades se deducen del pago a cuenta, pagos parciales o del pago final, según corresponda. Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD CONTRATANTE puede resolver el contrato por incumplimiento.

Conforme lo establece el numeral 229.2 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF la suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

2.16 OTRAS PENALIDADES

A fin de garantizar el cumplimiento optimo del servicio, a continuación, detallaremos las diferentes acciones y sus respectivas consecuencias en caso de incumplimiento de los SLA en los tiempos de respuesta On-line definidos.

<table>
<tr><th colspan="4">Otras penalidades</th></tr>
<tr><th>N°</th><th>Supuestos de aplicación de penalidad</th><th>Forma de cálculo</th><th>Procedimiento de verificación</th></tr>
<tr><td>1</td><td>Entre el 90% y 95% (*)</td><td>10% del importe mensual del servicio.</td><td rowspan="3">La Oficina de Tecnología de la Información realizará el seguimiento y verificación de los entregables de acuerdo con lo indicado en los términos de referencia y, ante algún incumplimiento trasladará comunicación mediante memorándum y/o informe a la Coordinación de Programación y Seguimiento del Departamento de Logística, precisando el supuesto incurrido para que este traslade y solicite a través de carta al contratista sus descargos, otorgándole un plazo de hasta 2 días calendario contabilizados a partir del día siguiente de notificado el supuesto de aplicación.

La Oficina de Tecnología de la Información tendrá 2 días calendario para evaluar el descargo, contabilizado a partir de recepcionado por el FMV.

La decisión tomada se hará de conocimiento al Departamento de Logística, a fin de que este en el plazo de 02 días calendario notifique al contratista la aplicación o no de la penalidad.</td></tr>
<tr><td>2</td><td>Entre el 80% y 89.99% (*)</td><td>20% del importe mensual del servicio.</td></tr>
<tr><td>3</td><td>Menos del 80% (*)</td><td>50% del importe mensual del servicio.</td></tr>
</table>

(*) Porcentaje de tickets atendidos según los SLA, en el período.

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

Las penalidades se deducen del pago a cuenta, pagos parciales o del pago final, según corresponda. Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD CONTRATANTE puede resolver el contrato por incumplimiento.

Conforme lo establece el numeral 229.2 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF la suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

2.17 RESOLUCIÓN CONTRACTUAL

a. <u>Resolución de contrato</u>

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral

68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

b. Cláusula de Cumplimiento (art. 8 de la Ley 31564)

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

c. Lineamiento corporativo de ética y conducta de FONAFE:

El prestador de servicios en general está obligado al cumplimiento de los principios y obligaciones establecidos en el "Lineamiento Corporativo de Ética y Conducta" de FONAFE, aprobado por Resolución de Dirección Ejecutiva N° 028-2021/DE-FONAFE con código N° 03.2.1.LC1 y versión 02, cuyo incumplimiento será considerado como causal de resolución de la presente contratación.

2.18 SANCIONES

La potestad de imponer sanción a proveedores, participantes, postores, contratistas y subcontratistas, referida en el artículo 88 de la Ley, por infracción a la Ley y el Reglamento, recae en el TCP. También le corresponde imponer sanciones en regímenes especiales de contratación, cuando dichas normas le atribuya expresamente esa potestad.

2.19 OBLIGACIÓN ANTICORRUPCIÓN

- **Anticorrupción y Antisoborno, conforme Ley 32069 y Reglamento:**

  EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

  Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

  Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[2] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

[2] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

e

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[3]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[4]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[5].

- **Prevención del lavado de activos y del financiamiento del terrorismo:**

  1) **EL PROVEEDOR**, sus socios, accionistas, asociados, aportantes, directores, representantes, funcionarios, empleados, asesores, agentes o, y/o personas vinculadas, en adelante "los Vinculados", declaran conocer las normas peruanas en materia de prevención del lavado de activos y del financiamiento del terrorismo y, por consiguiente, se obligan a presentar a EL FONDO la información y/o documentación que le sea solicitada para su adecuada identificación y la de sus "Vinculados", conforme a sus políticas y procedimientos para la prevención y gestión de los riesgos de lavado de activos y del financiamiento del terrorismo.

  2) **EL PROVEEDOR** declara que ella y/o sus vinculados no han sido condenados en el país o en el extranjero, mediante sentencia consentida o ejecutoriada por la comisión del delito de lavado de activos, financiamiento del terrorismo y/o delitos precedentes o equivalentes; asimismo, que no tienen mandato de prisión preventiva vigente o que, directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de los delitos antes mencionados, ante alguna autoridad nacional o extranjera competente.

  3) **EL PROVEEDOR** se obliga a poner en conocimiento inmediato de EL FONDO cualquier cambio referente a los antecedentes antes mencionados, que se produjeran con posterioridad a la firma del presente Contrato, de lo contrario se presumirá que no ha se ha producido ningún cambio en lo anteriormente declarado, sin perjuicio de lo estipulado en el siguiente párrafo.

  4) **EL PROVEEDOR** acepta expresamente que la falsedad a estas declaraciones o la omisión de comunicación de información o la negativa a proporcionar la información y/o documentación solicitada implica un incumplimiento sustancial del presente Contrato y, por consiguiente, su ocurrencia dará lugar a la resolución automática del mismo.

  5) En caso EL FONDO incurriera en costos y/o multas establecidas por una resolución administrativa o sentencia judicial firme, como consecuencia del incumplimiento de lo establecido en la presente clausula, **EL PROVEEDOR** se hará totalmente responsable por dichas multas y/o penalidades y/o

[3] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[4] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas
[5] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

indemnizaciones y/o pagos similares, asumiendo el importe de las mismas, sin reserva ni limitación alguna.

2.20 APLICACIÓN SUPLETORIA

La Ley 32069 prevalece sobre las normas del procedimiento administrativo general, de derecho público y sobre aquellas de derecho privado que sean aplicables, salvo en el caso de los procedimientos administrativos sancionadores a cargo del Tribunal de Contrataciones Públicas, y de los procedimientos administrativos sancionadores a cargo del OECE respecto de las infracciones de instituciones arbitrales y centros de administración de juntas de prevención y resolución de disputas; así como en el caso de los contratos estandarizados que se regulan conforme a sus cláusulas. Son de aplicación supletoria a los regímenes especiales de contratación siempre que no resulten incompatibles con tales normas especiales, sin perjuicio de la aplicación de los principios de la presente ley.

La conciliación y el arbitraje, en materia de contratación pública, se regulan especialmente por lo establecido en la presente ley y su reglamento, y se sujetan supletoriamente.

2.21 MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DE LA CONTRATACIÓN

Para ingresar a las instalaciones del FONDO MIVIVIENDA S.A. el proveedor deberá de contar con las siguientes medidas de seguridad:

- El FMV promueve el uso facultativo de mascarillas (obligatorio en caso de enfermedades respiratorias), la vacunación contra la COVID-19 y otras medidas de promoción y vigilancia de prácticas saludables y sanitarias; para lo cual el Ministerio de Salud, mediante Resolución Ministerial dicta las disposiciones que resulten necesarias.

- Es por cuenta y responsabilidad tener vigente su Constancia de Salud y Pensión de SCTR o un seguro particular, el cual deberá presentarlo cuando corresponda que algún personal del proveedor ingrese a las instalaciones del FMV. En caso de accidentes del personal, el proveedor asumirá el costo total de sus atenciones médico y/o quirúrgico, no siendo la responsabilidad del Fondo MIVIVIENDA S.A.

2.22 SOLUCIÓN DE CONTROVERSIAS

a. Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, conforme lo establecido en el Artículo 330 del reglamento del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009- 2025-EF.

b. Para la conciliación, el postor ganador de la buena pro selecciona a uno de las siguientes Instituciones de Conciliación para administrar la conciliación:

- El Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú
- Centro de Conciliación CECONSIL

2.23 OTRAS CLAUSULAS DE ANEXO:

a. Garantías:

Conforme lo señalado en Artículo 139 del Reglamento de la Ley General de Contrataciones Públicas - Ley Nº 32069 no corresponde otorgar garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias en los siguientes casos:

a) En los contratos de bienes y servicios cuyos montos sean menores o iguales a 50 UIT. Esta excepción no aplica cuando la sumatoria de los contratos derivados de procedimientos de selección por relación de ítems, adjudicados a un mismo postor, superen el monto señalado.

b) Contratos de arrendamiento de bienes muebles y bienes inmuebles de propiedad privada.

c) Las contrataciones complementarias que no superen el monto señalado en el literal a).

b. Gestión de riesgos:

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

c. Sistema de entrega

No aplica sistema de entrega para la presente contratación.

d. Subcontratación

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

e. Formula(s) de reajuste

No aplica formula de reajuste para la presente contratación.