Firmado digitalmente por ARAUJO CUADROS Klaus Joseph FAU 20131023414 hard
Motivo: Doy V° B°
Fecha: 26.06.2026 15:34:50 -05:00

# TÉRMINOS DE REFERENCIA

| | |
|---|---|
| Órgano y/o Unidad Orgánica: | OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES |
| Actividad del POI | AOI00015400158: ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA |
| Meta presupuestal | 057 |
| Denominación de la Contratación: | SERVICIO DE SUSCRIPCION DE PROTECCION AVANZADA ANTIMALWARE CON EDR Y SISTEMA DE ALERTAS INTEGRADO |

## 1. FINALIDAD PÚBLICA

La presente contratación tiene por finalidad fortalecer la seguridad de los servidores y equipos informáticos del Ministerio de Trabajo y Promoción del Empleo (MTPE), mediante la implementación de una solución de protección contra malware y ransomware, a fin de prevenir incidentes de seguridad que puedan comprometer la disponibilidad, integridad y confidencialidad de la información institucional.

Asimismo, la contratación contribuirá a garantizar la continuidad operativa de los sistemas de información y servicios digitales que brinda el MTPE a la ciudadanía, reduciendo los riesgos asociados a amenazas cibernéticas que puedan afectar el normal funcionamiento de la infraestructura tecnológica institucional.

## 2. OBJETIVO DE LA CONTRATACIÓN

### Objetivo General

Contratar la suscripción de una solución de protección contra malware y ransomware para los servidores y endpoints del Ministerio de Trabajo y Promoción del Empleo (MTPE), con la finalidad de fortalecer la seguridad de la infraestructura tecnológica institucional y reducir los riesgos asociados a amenazas cibernéticas que puedan afectar la continuidad de los servicios informáticos y la información institucional.

### Objetivos Específicos

- **Fortalecer la protección de la infraestructura tecnológica:** Implementar una solución de seguridad que permita prevenir, detectar y mitigar amenazas informáticas que afecten a los servidores y equipos de usuario final del MTPE.

- **Proteger los activos de información institucional:** Salvaguardar la información procesada y almacenada en la infraestructura tecnológica frente a incidentes de malware, ransomware y otras amenazas que comprometan su confidencialidad, integridad y disponibilidad.

- **Mejorar la capacidad de respuesta ante amenazas:** Contar con mecanismos de monitoreo y protección que permitan identificar oportunamente comportamientos maliciosos y reducir el impacto de posibles incidentes de seguridad.

- **Contribuir a la continuidad operativa de los servicios tecnológicos:** Minimizar el riesgo de interrupciones en los sistemas de información y

Firmado digitalmente por FIGUEROA HERNANDEZ Julio Gerardo FAU 20131023414 soft
Motivo: Doy V° B°
Fecha: 26.06.2026 11:26:55 -05:00



Firmado digitalmente por RODRIGUEZ CHAVEZ Aldo Marino FAU 20131023414 soft
Motivo: Doy V° B°
Fecha: 26.06.2026 11:39:38 -05:00

servicios digitales institucionales mediante la protección de los servidores y endpoints que forman parte de la plataforma tecnológica del MTPE.

## 3. ALCANCES O DESCRIPCIÓN DEL SERVICIO

La presente contratación comprende la suscripción de mil seiscientas sesenta y cuatro (1,664) licencias de una solución de protección contra malware y ransomware para servidores y endpoints del Ministerio de Trabajo y Promoción del Empleo (MTPE), incluyendo su implementación, configuración inicial, soporte técnico y acceso a actualizaciones durante el período de vigencia contractual.

La solución deberá permitir la protección de los activos informáticos institucionales comprendidos en el alcance del servicio, mediante mecanismos de prevención, detección y mitigación de amenazas informáticas que puedan afectar los sistemas operativos, aplicaciones y datos alojados en servidores y equipos de usuario final.

**Cuadro N.° 01 – Elementos técnicos considerados para la prestación del servicio**

| N.° | Descripción | Unidad de Medida | Cantidad |
|---|---|---|---|
| 01 | Suscripción de licencias de protección contra malware y ransomware para servidores y endpoints, con capacidad de detectar y responder ante incidentes, incluyendo acceso a actualizaciones, soporte técnico del fabricante e implementación de la solución. | Servicio | 01 |

La solución deberá proporcionar capacidades de protección contra malware, ransomware y otras amenazas informáticas que puedan afectar a los servidores y endpoints comprendidos en el alcance del servicio, permitiendo su administración centralizada mediante una consola de gestión.

Asimismo, el postor podrá incluir funcionalidades adicionales que fortalezcan las capacidades de protección, administración o monitoreo de la solución ofertada, siempre que estas no generen costos adicionales para la Entidad ni requieran licenciamiento, infraestructura o componentes adicionales no contemplados en el presente requerimiento.

### 3.1. Infraestructura tecnológica comprendida en el servicio

La presente contratación comprende la protección de la infraestructura tecnológica institucional administrada por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), conformada por servidores y equipos de usuario final (endpoints), de acuerdo con el inventario de activos informáticos vigente.

La solución ofertada deberá ser compatible con los sistemas operativos y cantidades detalladas a continuación, considerando la totalidad de activos comprendidos en el alcance del servicio.

#### a) Servidores

| | |
|---|---|

| Sistema Operativo | Cantidad |
|---|---|
| CentOS Linux (versiones 7.x) | **72** |
| Red Hat Enterprise Linux (versiones 8.x) | **25** |
| Oracle Linux (versiones 7.x y 8.x) | **30** |
| Windows Server (2012, 2016, 2019, 2022) | **27** |
| **Subtotal servidores** | **154** |

**b) Endpoints**

| Tipo de equipo | Sistema Operativo | Cantidad |
|---|---|---|
| Laptops | Windows 10 / 11 | **194** |
| Equipos integrados | Windows 11 | **826** |
| PCs | Windows 10 / 11 | **464** |
| Equipos Apple | macOS | **5** |
| Pc´s transferidos de la unidad ejecutora Fortalece | Windows 10 / 11 | **21** |
| **Subtotal endpoints** | | **1,510** |

**c) Total, de licencias requeridas**

| Concepto | Cantidad |
|---|---|
| Servidores | **154** |
| Endpoints | **1,510** |
| **TOTAL, GENERAL** | **1,664** |

La cantidad de licencias requerida ha sido determinada en función del inventario institucional vigente y corresponde a la totalidad de servidores y endpoints que serán protegidos por la solución objeto de la presente contratación.

## 3.2. Características técnicas mínimas de la solución

La solución ofertada deberá proporcionar protección para la totalidad de los activos informáticos comprendidos en el presente requerimiento, garantizando compatibilidad con los sistemas operativos detallados en el inventario institucional y permitiendo una administración centralizada de la seguridad.

Asimismo, la solución deberá cumplir, como mínimo, con las características técnicas señaladas en el Cuadro N.° 02, las cuales deberán ser acreditadas mediante brochure, ficha técnica, datasheet o documentación oficial emitida por el fabricante. En caso la información no se encuentre expresamente indicada en la documentación técnica presentada, el postor podrá complementarla mediante carta del fabricante o representante autorizado.

**Cuadro N.° 02 – Características técnicas mínimas y forma de acreditación**

| N.° | Característica técnica mínima |
|---|---|
| 1 | Contar con una administración basada en la nube (SaaS) o |

| N.° | **Característica técnica mínima** |
|---|---|
| | arquitectura equivalente. |
| 2 | Protección contra malware y ransomware y protección contra amenazas de día cero (Zero-Day) mediante análisis de comportamiento, inteligencia artificial o tecnología equivalente (deseable). |
| 3 | Protección contra exploits anticipándose a los ataques sobre vulnerabilidades. |
| 4 | Consola centralizada de administración con doble factor de autenticación. |
| 5 | Protección deberá poder permitir ingresas hash o MD5 para crear listas legras de aplicaciones en la red. |
| 6 | Compatibilidad con Windows 10 y Windows 11. |
| 7 | Compatibilidad con Windows Server 2016 o superior. |
| 8<br>9 | Compatibilidad con Linux (CentOS, Red Hat Enterprise Linux y Oracle Linux o equivalentes). |
| 10 | Actualización automática de firmas, motores de detección y componentes de seguridad. |
| 11 | Gestión de políticas de seguridad desde consola centralizada. |
| 12 | Control y/o administración de dispositivos USB o almacenamiento externo. |
| 13 | Protección contra alteración o deshabilitación no autorizada del agente de seguridad (Anti-Tamper o equivalente). |
| 14 | Generación de alertas y eventos de seguridad basado en incidentes permitiendo asignar responsable, definir criticidad y marcar estado. |
| 15 | Capacidad de generar reportes de seguridad desde la consola de administración. |
| 16 | Detección pre-ejecución con machine learning ajustable<br>La solución debe incluir una capa de detección pre-ejecución basada en modelos de machine learning locales, con al menos tres niveles de agresividad configurables por el administrador (normal, agresivo, tolerante), operativos sin conexión a la nube y sin requerir actualizaciones de firmas para su funcionamiento. |
| 17 | Análisis de riesgo de configuración por endpoint, la plataforma debe calcular y presentar un índice de riesgo individual por endpoint basado en configuraciones incorrectas, aplicaciones vulnerables, comportamientos del usuario y estado de parches, con capacidad de ordenar y filtrar el parque de endpoints por nivel de riesgo y generar recomendaciones de remediación automática. |
| 18 | Árbol de procesos completo con trazabilidad forense, ante cualquier evento de detección, la solución debe presentar el árbol de procesos completo (proceso raíz → padre → hijo → nieto) con los siguientes atributos por nodo: hash SHA-256, ruta absoluta, línea de comandos completa, PID, usuario autenticado, hora de inicio y conexiones de red asociadas al proceso en el momento de ejecución. |
| 19 | Detección basada en indicadores de ataque (IOA) sin malware, la solución debe detectar técnicas de ataque que no involucran archivos maliciosos (fileless attacks, LOLBins, living-off-the-land), utilizando análisis de comportamiento en tiempo real basado en IOA (Indicators of Attack), independientemente de si existe un archivo ejecutable que |

| N.° | **Característica técnica mínima** |
|---|---|
| | pueda ser analizado por hash o firma. |
| 20 | Sandbox integrado con detonación local y en nube<br>La plataforma debe incluir un módulo de sandbox capaz de detonar archivos sospechosos tanto en entorno local (on-premise) como en infraestructura cloud del fabricante, con soporte para análisis de archivos ejecutables PE, scripts (PowerShell, VBScript, JavaScript), documentos Office con macros y archivos PDF, entregando un reporte de comportamiento con IOC extraídos. |
| 21 | Aislamiento de endpoint con canal de comunicación administrativo preservado, la solución debe permitir el aislamiento de red de un endpoint comprometido desde la consola central, cortando toda conectividad con la red corporativa e internet, pero preservando el canal de comunicación cifrado entre el agente y la consola de administración para permitir la continuación de la investigación forense y la ejecución de comandos remotos durante el aislamiento. |
| 22 | Ejecución remota de comandos y scripts en endpoint aislado.<br>Durante o fuera del aislamiento, la consola debe permitir la ejecución remota de comandos y scripts en el endpoint desde la consola central sin requerir conexión RDP, VPN ni herramientas de terceros, con registro de auditoría completo de cada comando ejecutado, el analista que lo ejecutó y el resultado obtenido. |
| 23 | Correlación XDR multifuente con puntuación de incidente<br>La plataforma debe correlacionar eventos provenientes de al menos cuatro fuentes distintas (endpoint, red, identidad, correo electrónico o nube) para construir incidentes unificados con una puntuación de severidad calculada automáticamente, agrupando eventos relacionados en una sola vista de investigación en lugar de alertas individuales. |
| 24 | Control granular de dispositivos externos con políticas por contexto<br>La plataforma debe permitir la definición de políticas de control de dispositivos externos (USB, Bluetooth, dispositivos de almacenamiento, impresoras) con granularidad por tipo de dispositivo, vendor ID, product ID, número de serie, usuario y grupo de Active Directory, con capacidad de permitir solo lectura, bloqueo total o acceso controlado según el contexto. |
| 25 | Protección de memoria contra técnicas de inyección y evasión<br>La solución debe incluir protección activa de memoria en tiempo de ejecución, capaz de detectar y bloquear técnicas de inyección de código (process hollowing, DLL injection, reflective DLL loading, APC injection) y técnicas de evasión de EDR (patch de funciones NTDLL, unhooking, direct syscalls), sin depender exclusivamente de firmas o hashes conocidos. |
| 26 | Rollback automático de cambios ante detección de ransomware<br>La plataforma debe incluir capacidad de revertir automáticamente los cambios realizados por un proceso identificado como ransomware (archivos cifrados, modificaciones de registro, cambios en el MBR), restaurando los archivos afectados a su estado previo al ataque, con un registro detallado de los archivos recuperados y los que no pudieron ser restaurados. |
| 27 | Consola de administración unificada multi-tenant con delegación de roles<br>La solución debe operar bajo una consola única que gestione todos los módulos de seguridad (antivirus, EDR, XDR, control de dispositivos, |

| N.° | **Característica técnica mínima** |
|---|---|
| | cifrado, gestión de vulnerabilidades) sin consolas separadas por módulo, con soporte para arquitectura multi-tenant, delegación de roles administrativos por grupos de endpoints y registro de auditoría de todas las acciones administrativas. |
| 28 | Integración con SIEM mediante API REST y syslog estructurado<br>La plataforma debe exponer una API REST documentada y soportar envío de eventos por syslog en formato estructurado (JSON), con campos normalizados que incluyan como mínimo: tipo de evento, host origen, proceso involucrado, usuario, hash, técnica MITRE ATT&CK asociada, severidad y acción tomada, permitiendo la integración con plataformas SIEM sin desarrollos intermedios propietarios. |
| 29 | Mapeo nativo de detecciones al marco MITRE ATT&CK<br>Cada detección generada por la plataforma debe incluir el mapeo automático a la táctica y técnica correspondiente del marco MITRE ATT&CK (versión vigente), visible desde la consola sin configuración adicional, con capacidad de filtrar y buscar incidentes por táctica, técnica o subtécnica específica. |
| 30 | Análisis de riesgo de identidad y comportamiento de usuario<br>La solución debe evaluar el riesgo asociado a cuentas de usuario mediante el análisis de comportamiento (UEBA), detectando anomalías tales como accesos en horarios inusuales, escalación de privilegios no autorizada, uso de credenciales en múltiples endpoints simultáneamente y acceso a recursos fuera del patrón histórico del usuario, generando una puntuación de riesgo de identidad actualizada en tiempo real. |
| 31 | Soporte de agente unificado para sistemas operativos heterogéneos<br>La solución debe operar mediante un agente único que soporte de forma nativa, sin módulos adicionales de terceros, las siguientes plataformas: Windows (versiones 10, 11 y Server 2016/2019/2022), macOS (últimas tres versiones mayores) y distribuciones Linux (Ubuntu 20.04+, CentOS/RHEL 7+, Debian 10+), con paridad de funcionalidades EDR entre plataformas. |
| 32 | Retención de telemetría forense con búsqueda retroactiva<br>La plataforma debe retener la telemetría de eventos de endpoint (procesos, conexiones de red, modificaciones de archivos y registro) por un período mínimo de 90 días, con capacidad de búsqueda retroactiva mediante consultas sobre esa telemetría histórica para identificar si un indicador de compromiso (IOC) recién descubierto estuvo presente en la red antes de ser conocido (threat hunting retrospectivo). |
| 33 | La plataforma se deberá integrar a un SOAR que permita la generación de alertas de ciberseguridad en el contexto del EDR en tiempo real. |
| 34 | La plataforma debe estar integrada a un sistema de automatización de procesos creando tickets y ejecutando flujos de atención predeterminados a fin de documentar el cumplimiento de SLAs de respuesta. |

Todas las características técnicas mínimas señaladas en el Cuadro N.° 02 deberán acreditarse mediante brochure, ficha técnica, datasheet, documentación oficial emitida por el fabricante o carta del fabricante o representante autorizado. En caso la información no se encuentre

expresamente indicada en la documentación técnica presentada, podrá ser complementada mediante carta emitida por el fabricante o representante autorizado.

## 4. REQUISITOS DEL PROVEEDOR Y DEL PERSONAL PROPUESTO

### 4.1. PERFIL DEL PROVEEDOR:

- Persona natural o jurídica.
- Contar con RUC activo y habido.
- Contar con inscripción vigente en el Registro Nacional de Proveedores (RNP) en el capítulo de Bienes y/o Servicios, según corresponda.
- No encontrarse impedido, suspendido ni inhabilitado para contratar con el Estado.

### 4.2. EXPERIENCIA DEL POSTOR:

El proveedor deberá acreditar experiencia en la prestación de servicios vinculados a soluciones de seguridad informática.

Deberá acreditar una experiencia acumulada mínima de S/ 80,000.00 (Ochenta mil con 00/100 soles), correspondiente a servicios iguales o similares al objeto de la contratación, ejecutados durante los últimos cinco (05) años.

**Contrataciones Similares**

Se consideran servicios similares, entre otros, los siguientes:

- Servicios de suscripción de software de seguridad informática.
- Servicios de protección contra malware, ransomware y otras amenazas informáticas.
- Servicios de administración, monitoreo o gestión de plataformas de seguridad informática.
- Servicios de licenciamiento o suscripción de software de seguridad, EDR o XDR.
- Servicios de implementación, soporte, actualización o suscripción de software de seguridad lógica.

**Forma de acreditación**

La experiencia se acreditará mediante contratos u órdenes de servicio y su respectiva conformidad o constancia de prestación; o comprobantes de pago cuya cancelación se acredite documental y fehacientemente mediante voucher de depósito, nota de abono, reporte de estado de cuenta o cualquier otro documento emitido por entidad del sistema financiero que acredite el abono correspondiente.

### 4.3. DEL PERSONAL PROPUESTO.

**No aplica**

## 5. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

El servicio será prestado para la infraestructura tecnológica del Ministerio de Trabajo y Promoción del Empleo (MTPE), ubicada en la Av. Salaverry N.° 655, distrito de Jesús María, provincia y departamento de Lima.

La implementación, configuración y administración de la solución podrá realizarse de manera remota y/o presencial, según lo requiera la Entidad, comprendiendo los servidores y endpoints incluidos en el alcance del servicio.

### 5.1. Plazo de Ejecución:

El contratista contará con un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de notificada la Orden de Servicio, para realizar la implementación, configuración inicial y activación de las licencias de la solución.

Concluida la implementación y validado el correcto funcionamiento de la solución, se suscribirá el Acta de Implementación e Inicio del Servicio.

La vigencia de la suscripción será de noventa (90) días calendario, contados a partir del día siguiente de la suscripción del Acta de Implementación e Inicio del Servicio.

Asimismo, el contratista deberá presentar el entregable correspondiente a la implementación y activación de la solución dentro de los cinco (05) días calendario siguientes a la suscripción del Acta de Implementación e Inicio del Servicio.

## 6. ENTREGABLE

El contratista deberá presentar un único entregable que acredite la implementación, activación y puesta en operación de la solución objeto de la contratación.

El entregable deberá ser presentado a través de la Mesa de Partes física o virtual del Ministerio de Trabajo y Promoción del Empleo (MTPE), conforme a los procedimientos vigentes de la Entidad.

### 6.1. Documentos a presentar y plazo

El contratista deberá presentar, dentro de los cinco (05) días calendario posteriores a la suscripción del Acta de Implementación e Inicio del Servicio, como mínimo la siguiente documentación:

**a.** Certificado de licencia que acredite la activación de la suscripción de las mil seiscientas sesenta y cuatro (1,664) licencias de protección contra malware y ransomware a nombre del Ministerio de Trabajo y Promoción del Empleo (MTPE), indicando la vigencia correspondiente.

**b.** Acta de Implementación e Inicio del Servicio, suscrita por el representante del contratista y el responsable designado por la Entidad, donde conste la implementación, configuración inicial y puesta en operación de la solución.

**c.** Informe técnico de implementación, que contenga como mínimo:
- Descripción de las actividades ejecutadas.
- Cantidad de licencias activadas.
- Relación de servidores y endpoints incorporados a la solución.
- Evidencia de funcionamiento de la consola de administración.

- Fecha de inicio y fecha de término de la vigencia de la suscripción.

**6.2. Modalidad de Presentación.**

El entregable deberá ser presentado a través de la Mesa de Partes física o virtual del MTPE, conforme a los procedimientos establecidos por la Entidad.

En caso de presentación virtual, la documentación deberá remitirse a través de la Mesa de Partes Digital del MTPE, a través del siguiente enlace: https://mesadigital360.trabajo.gob.pe/

## 7. CONFORMIDAD DEL SERVICIO

La conformidad de la prestación del servicio se regirá por lo dispuesto en el artículo 144 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas.

La conformidad será otorgada por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC) de la Oficina General de Estadística y Tecnologías de la Información (OGETIC), previa verificación del cumplimiento de las condiciones y obligaciones establecidas en los presentes Términos de Referencia.

Para efectos de la conformidad, se verificará la presentación y aprobación del entregable correspondiente, así como la suscripción del Acta de Implementación e Inicio del Servicio, debidamente firmada por las partes.

## 8. FORMA DE PAGO

El pago se realizará en un único pago, previa conformidad de la prestación por parte de la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), de acuerdo con las condiciones establecidas en los presentes Términos de Referencia.

8.1. **Condiciones para el pago:**

El pago se efectuará una vez cumplidos los siguientes requisitos:

- Implementación, configuración inicial y activación de las mil seiscientas sesenta y cuatro (1,664) licencias de protección contra malware y ransomware para servidores y endpoints del MTPE.

- Presentación del entregable establecido en el numeral 6 de los presentes Términos de Referencia.

- Suscripción del Acta de Implementación e Inicio del Servicio.

- Emisión de la conformidad por parte de la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), previa verificación del cumplimiento de las obligaciones contractuales.

## 9. PENALIDAD APLICABLES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad aplicará automáticamente la penalidad por mora por cada día calendario de atraso que le sea imputable, de conformidad con

lo dispuesto en el artículo 120 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas.
La penalidad diaria se calculará de acuerdo con la siguiente fórmula:

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

Donde:
F = 0.40 para bienes y servicios.
La aplicación de la penalidad por mora se efectuará conforme a las disposiciones establecidas en el artículo 120 del Reglamento de la Ley N.° 32069, Ley General de Contrataciones Públicas.

**Otras penalidades**
No corresponde.

## 10. SEGURIDAD DE LA INFORMACIÓN

El contratista deberá mantener estricta reserva y confidencialidad respecto de toda la información, documentación, configuraciones, credenciales, registros, reportes y demás datos a los que tenga acceso con ocasión de la prestación del servicio, comprometiéndose a no divulgar, reproducir, transferir o utilizar dicha información para fines distintos a los establecidos en la presente contratación.

La información obtenida durante la implementación, configuración, administración, soporte o cualquier otra actividad relacionada con el servicio deberá ser utilizada exclusivamente para la ejecución de las prestaciones contratadas, incluso después de culminada la vigencia contractual.

Asimismo, el contratista deberá cumplir con las disposiciones contenidas en la Política de Seguridad de la Información del MTPE vigente, así como con la normativa aplicable en materia de Seguridad Digital, Protección de Datos Personales y demás disposiciones que resulten aplicables durante la ejecución del servicio.

En caso de identificar vulnerabilidades, incidentes de seguridad, accesos no autorizados o cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de la información o de los activos tecnológicos de la Entidad, el contratista deberá comunicarlo de manera inmediata a la Oficina de Tecnologías de la Información y Comunicaciones (OTIC) y al Oficial de Seguridad y Confianza Digital del MTPE, para la adopción de las acciones correspondientes.

## 11. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la calidad de la prestación del servicio y por los vicios ocultos que pudieran presentarse como consecuencia de la implementación, configuración, activación o funcionamiento de la solución objeto de la contratación, por un período de un (01) año, contado a partir de la conformidad otorgada por la Entidad.

Se consideran vicios ocultos aquellas deficiencias no detectables al momento de otorgarse la conformidad y que afecten el correcto funcionamiento de la solución implementada, tales como:

- Errores de configuración que comprometan la operatividad de la solución.
- Deficiencias en la implementación o activación de las licencias contratadas.
- Fallas atribuibles a la implementación realizada por el contratista que afecten las capacidades de protección de la solución.
- Omisiones o defectos en la configuración que impidan el adecuado funcionamiento de la consola de administración o de los agentes instalados.
- Cualquier otra deficiencia imputable al contratista que no haya podido ser advertida durante la evaluación para la conformidad del servicio.

En caso de presentarse alguno de los supuestos señalados, el contratista deberá efectuar las correcciones, ajustes, reconfiguraciones o acciones necesarias para restablecer el correcto funcionamiento de la solución, sin costo adicional para el Ministerio de Trabajo y Promoción del Empleo.

## 12. RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes podrá resolver el contrato, de conformidad con lo establecido en la Ley N.° 32069 – Ley General de Contrataciones Públicas, su Reglamento aprobado mediante Decreto Supremo N.° 009-2025-EF y la Directiva N.° 005-2025-MTPE/4, que regula la contratación de bienes y servicios bajo la modalidad de contratos menores en el Ministerio de Trabajo y Promoción del Empleo – Unidad Ejecutora 001 – Oficina General de Administración.

Constituyen causales de resolución contractual las siguientes:

**a)** Caso fortuito o fuerza mayor que imposibilite la continuación de la contratación.
**b)** Incumplimiento de las obligaciones contractuales por causa atribuible al contratista.
**c)** Hecho sobreviniente al perfeccionamiento del contrato menor, distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuidad de la contratación.
**d)** Incumplimiento de la cláusula anticorrupción y antisoborno.
**e)** Presentación de documentación falsa, adulterada o con información inexacta en cualquier etapa del proceso de contratación o durante la ejecución contractual.
**f)** Configuración de la condición de terminación anticipada establecida en el contrato menor u Orden de Servicio.

Asimismo, constituye causal de resolución contractual la presentación de información falsa o inexacta en la Declaración Jurada de Prohibiciones e Incompatibilidades prevista en la Ley N.° 31564 – Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.

En caso de verificarse el incumplimiento de los impedimentos establecidos en el artículo 5 de la referida Ley, corresponderá la aplicación de las sanciones y medidas previstas en la normativa vigente, incluida la inhabilitación para contratar o prestar servicios al Estado, de corresponder.

## 13. ANTICORRUPCIÓN Y ANTISOBORNO

El contratista declara y garantiza que no ha ofrecido, prometido, entregado ni efectuado, directa o indirectamente, pago, beneficio o incentivo indebido alguno a funcionarios, servidores o terceros vinculados al Ministerio de Trabajo y Promoción del Empleo (MTPE), con la finalidad de obtener ventajas en el proceso de contratación o durante la ejecución contractual.

Asimismo, se compromete a actuar con integridad, transparencia y respeto a la normativa vigente, absteniéndose de realizar cualquier acto de corrupción o soborno durante la ejecución de la prestación.

El incumplimiento de lo establecido en el presente numeral facultará a la Entidad a adoptar las acciones correspondientes, incluyendo la resolución contractual, de ser el caso.

El contratista declara conocer y cumplir las disposiciones contenidas en la Ley N.° 27815, Ley del Código de Ética de la Función Pública, y demás normas aplicables en materia de integridad y lucha contra la corrupción.

## 14. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato o la orden de servicio se resolverán mediante conciliación, con excepción de aquellas que versen sobre nulidad de contrato, conforme a lo dispuesto en el numeral 81.3 del artículo 81 de la Ley N.° 32069, Ley General de Contrataciones Públicas.

Sin perjuicio de lo anterior, en caso de no arribar a un acuerdo conciliatorio, las controversias surgidas durante la ejecución del contrato serán resueltas en la vía arbitral o a través de la jurisdicción ordinaria, según el acuerdo de las partes. A falta de acuerdo, dichas controversias serán sometidas a la jurisdicción de los jueces y tribunales del Distrito Judicial de Lima.

## 15. GESTIÓN DE RIESGOS

Las partes realizan la gestión de riesgos con el objetivo de tomar decisiones informadas y disminuir la probabilidad de impactos negativos durante la ejecución del contrato, considerando la finalidad pública de la contratación.

| Descripción del Riesgo | Prioridad del Riesgo | Riesgo Asignado | |
|---|---|---|---|
| | | Entidad | Contratista |
| Retraso en la implementación, configuración o activación de las licencias por causas atribuibles al contratista. | Alto | | X |
| Incompatibilidad de la solución ofertada con alguno de los sistemas operativos comprendidos en el alcance del servicio. | Muy Alto | | X |
| Activación incompleta o incorrecta de las licencias contratadas. | Muy Alto | | X |

| | | | |
|---|---|---|---|
| Afectación de la operatividad de servidores o endpoints durante las actividades de implementación o configuración de la solución. | Alto | | X |
| Restricciones de acceso a los activos tecnológicos o limitaciones operativas que dificulten la implementación de la solución. | Medio | X | |
| Incidentes relacionados con la seguridad de la información o acceso no autorizado a información, configuraciones o activos tecnológicos de la Entidad. | Muy Alto | X | X |
| Variaciones en el inventario de activos informáticos durante la ejecución del servicio que requieran reasignación de licencias. | Medio | X | X |
| Indisponibilidad temporal de servicios del fabricante o de la plataforma de administración que afecte la activación o gestión de la solución. | Medio | | X |