Anexo N° 01-B

ESPECIFICACIONES TÉCNICAS

Órgano y/o Unidad Orgánica:	UNIDAD FUNCIONAL DE TECNOLOGIAS DE LA INFORMACION	
Actividad del POI/Acción Estratégica PEI:	AOI00106600144. GESTIÓN OPERATIVA – UFTI 5000276	
Cuadro Multianual de Necesidades	Meta	0018
	Código Siga	140400030825
Denominación de la Contratación:	ADQUISICIÓN DEL SISTEMA DE SEGURIDAD PARA LA PROTECCIÓN DEL SERVICIO DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN DE MICROSOFT OFFICE 365 PARA EL PROGRAMA DE EMPLEO TEMPORAL "LLAMKASUN PERÚ".	

I. FINALIDAD PÚBLICA

La presente adquisición tiene como finalidad lograr las metas y objetivos encargados al Programa de Empleo Temporal "LLamkasun Perú", por lo cual es necesaria contar con un sistema de protección de correo electrónico para prevenir posibles riesgos de ataques de virus, spam, phishing, malware y otros ataques informáticos que se propagan mediante el correo electrónico, permitiendo con ello una comunicación segura del Programa de Empleo Temporal "LLamkasun Perú".

II. OBJETIVO DE LA CONTRATACIÓN

Adquisición de un sistema de seguridad para la protección del servicio de correo electrónico y herramientas de colaboración de Microsoft office 365 para el Programa de Empleo Temporal "LLamkasun Perú", para la protección integral de los buzones del correo electrónico y las herramientas colaborativas de la institución manteniendo una comunicación segura ante cualquier ataque cibernético.

III. CARACTERÍSTICAS TÉCNICAS:

EL Programa "LLamkasun Perú" requiere adquirir un sistema antispam de acuerdo a las siguientes características:

ITEM	*DESCRIPCIÓN*	*CANTIDAD*	*UNIDAD DE MEDIDA*
01	*Sistema de seguridad de correos electrónicos en la nube*	*1*	*Unidad*

3.1. CARACTERÍSTICAS Y CONDICIONES DEL BIEN

Aspectos Generales de La Solución

- *Solución de seguridad integral para correo electrónico y aplicaciones de colaboración de Microsoft Office 365 en modalidad SaaS, con capacidad avanzadas de anti-phishing para correos entrantes y salientes, protección contra malware, protección de URL maliciosas (URL Sandboxing), capacidad de re-escritura de URLs y código QR, identificación de anomalías y de robo o compromiso de cuentas de usuario, para 400 cuentas de correo.*
- *El servicio debe operar desde la propia nube del fabricante de seguridad e integrarse de manera nativa y con capacidad de prevención en línea (in-line) mediante tecnologías API, en la nube del proveedor de servicios de correo electrónico y colaboración (Microsoft Office 365). No se*

PERÚ MTPE
Firmado digitalmente por GUZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:07:34 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 10:58:40 -05:00

aceptarán soluciones basadas en "Security Email Gateway" o similar, y no debe ser necesario ningún cambio disruptivo en el servicio de correo, tales como cambios de registro DNS (MX), relay SMTP, o cualquier otra modificación a nivel de tráfico SMTP que ingresa a la nube del Microsoft.

- *La solución de seguridad deberá poder proteger de amenazas cibernéticas en modalidad SaaS (Software as a Service) al servicio de Microsoft Office 365.*
- *La detección y prevención de amenazas para el correo electrónico debe ser tanto para el flujo entrante, saliente e interno (entre usuarios del mismo dominio o Tenant).*
- *La solución deberá proporcionar protección contra los siguientes ataques cibernéticos:*
  - *Amenazas de phishing.*
  - *Amenazas de Spam.*
  - *Amenazas de malware.*
  - *Protección contra URL maliciosas contenidas tanto en el cuerpo del mensaje, como en los archivos adjuntos.*
  - *Re-escritura o reemplazo de URLs contenidas tanto en el cuerpo del mensaje, como en los archivos adjuntos (Microsoft Office y Adobe PDF).*
  - *Identificación y alerta del uso de aplicaciones SaaS públicas no autorizadas.*
  - *Detección de Anomalías en el uso del correo y de robo de credenciales/cuentas.*
  - *Protección contra archivos protegidos o cifrados con contraseña.*
  - *Protección contra ataques de Phishign basado en códigos QR.*
- *La solución deberá poner en cuarentena los correos electrónicos y su contenido malicioso y ofrecerá al usuario opciones para eliminar los recursos en cuarentena o restaurarlos.*
- *La solución debe soportar la protección de las aplicaciones SaaS realizando "acciones de prevencion en línea" sobre los correos electrónicos, previniendo las amenazas antes de que estas lleguen a los buzones de correo de Office 365 del usuario final.*
- *La solución debe ser compatible con la conexión a la nube de "inteligencia de amenazas" del fabricante para compartir IoC (indicadores de compromiso) y actualizaciones de amenazas.*
- *La solución debe tener capacidad de análisis de DMARC (Domain-based Message Authentication, Reporting and Conformance) para rechazar o llevar a cuarentena de correos entrantes que fallan en DMARC.*
- *La solución debe tener capacidad para proteger NickName Impersonation, que es el ataque donde el ciber-delincuente se hace pasar por los nombres y correos electrónicos de los ejecutivos de la empresa para intentar engañar a un empleado interno para que revele información confidencial o ejecute algún pago. Se debe poder configurar la protección para cuentas estratégicas de la organización.*
- *La solución detectará y proporcionará informes de aplicaciones SaaS no reconocidas o autorizadas por los administradores (Shadow IT).*
- *La solución debe tener una pista de auditoria (audit trail) sobre todos los cambios realizados en la plataforma, indicando: fecha y hora del cambio, usuario que realizo, tipo de cambio y descripción asociada.*
- *La solución debe tener capacidades reportes detallados diarios hacia los usuarios finales, sobre su cuarentena o spam retenido en las últimas 24 horas.*
- *Los correos que fueron cuarentenados pueden ser liberados por el propio usuario final o solicitar su liberación al administrador (configurable basado en la política y flujo del evento de seguridad que lo origino).*

Capacidades requeridas de prevención de malware y phishing en Microsoft Office 365

- *La solución deberá emplear algoritmos entrenadas de Inteligencia Artificila para identificar phishing avanzado o phishing de dia-cero y compromiso en el correo electrónico (Bussines Email Compromise), tanto en el tráfico de correo entrante, saliente e interno.*
- *La solución deberá reconocer correos electrónicos de phishing basado en reputación de la URL (cuenta con referencia maliciosa) y emulación de URL (emula el sitio web para identificar phishing de día-cero).*
- *El motor Anti-Phishing debe analizar diferentes componentes de un correo electrónico, como son: los archivos adjuntos, los enlaces URL, la reputación del remitente, análisis de dominio, OCR y el idioma utilizado, empleando para ello un motor de Inteligencia Artificial y/o Machine Learning con soporte de múltiples idiomas (NLP - Natural Language Processing Engine o similar).*
- *Las capacidades de antimalware deben poder analizar todos los archivos que son cargados y compartidos en la nube de Office 365.*

PERÚ MTPE
Firmado digitalmente por QUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:07:53 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 10:58:57 -05:00

- *La solución debe tener capacidad de re-escritura de URLs para prevenir el phishing conocido y no conocido (phishing de día-cero). Debe tener las siguientes acciones:*
  - *Reemplazar los enlaces URL en el cuerpo del correo electrónico y en los archivos adjuntos (Microsoft Office y Adobe PDF). Los enlaces URL reemplazados deben direccionar a los servicios de inspección de seguridad del propio fabricante, de modo que cada vez que un usuario hace clic en un enlace, se inspecciona el sitio web detrás del enlace para asegurarse de que no sea un sitio web de phishing.*
  - *La capacidad de reemplazo de enlaces URL debe operar tanto en reputación URL, como en emulación de URL (URL Sandbox) parar detectar sitios web de phishing de día cero.*
  - *Debe tener capacidad forense. Debe registrar el momento que el usuario hace clic en el enlace reemplazado, con fines forenses y de auditoría, indicando el resultado del análisis y si el recurso de URL fue bloqueado para el usuario al momento del clic.*
  - *Sobre cada correo donde se reemplazaron los enlaces, debe tener la capacidad de ver los enlaces reemplazados, y la actividad del usuario sobre esos enlaces (User Clics).*
  - *La inspección de los enlaces URL, debe ser tanto basado en reputación (Se sabe que la URL es maliciosa o contiene referencias maliciosas), como en emulación (Emula el sitio web URL para detectar phishing de día cero).*
  - *La solución debe tener capacidad de detección ataques basados en códigos QR (enlaces que están detrás de códigos QR y fueron detectados como maliciosos) y facilitar la presentación de informes sobre estos tipos de ataques, indicando cuándo hay un enlace detrás de un código QR.*
- *La solución debe tener capacidad de re-escritura de los enlaces que se encuentan en el codigo QR que se incluye en cuerpo del mensaje, es decir, debe reemplazar el codigo QR con un nuevo codigo, el cual contenga un nuevo enlace para la prevención de ataques basados en códigos QR.*
- *La solución debe ofrecer protección contra archivos protegidos o cifrados con contraseña. En primera instancia, debe intentar extraer la contraseña obtenida en el cuerpo del correo electrónico. Si no se encuentra la contraseña, la solución debe permitir realizar las siguientes acciones configurables:*
  - *Requerir que el usuario final ingrese una contraseña. El archivo es removido del correo temporalmente, hasta que el usuario final ingrese la contraseña y el archivo pueda ser analizado y posteriormente liberado de ser el caso.*
  - *El usuario final recibe el correo con una alerta.*
  - *Cuarentena. El usuario recibe una alerta y se le permite restaurar el correo electrónico.*
  - *Cuarentena. El usuario no recibe una alerta (el administrador puede restaurar el correo).*
- *Para los archivos protegidos por contraseña o cifrados, debe soportar por lo menos los siguientes tipos de archivo: CAB, IMG, ISO, RAR, TAR, TAR.BZ2, TAR.GZ, ZIP, 7Z, Adobe PDF y Microsoft Office.*
- *La solución debe tener la posibilidad de enviar reportes semanales de estado de seguridad y utilización analítica, por cada aplicación SaaS que es protegida por la plataforma de seguridad.*
- *La solución debe tener una consola para realizar búsquedas de todos los correos electrónicos y las acciones de seguridad realizadas en cada uno de ellos. Sobre el resultado obtenido en la búsqueda, se debe tener capacidad de tomar acciones tales como: enviar a cuarentena o restaurar de cuarentena, crear "lista blanca" (allow-list) o "lista negra" (block-list).*
- *La solución debe tener una capacidad mínima de retención de los correos y sus metadatos, de acuerdo con lo siguiente:*
  - *Correo con amenazas sin cuarentena (correo original y adjuntos) de 14 dias.*
  - *Correo con amenazas sin cuarentena (metadatos y atributos) de 180 dias.*
  - *Correo en cuarentena (correo original y adjuntos) de 180 dias.*
  - *Correo en cuarentena (metadatos y atributos) de 180 dias.*

Capacidades requeridas de detección de comportamiento anómalo para identificar robo o compromiso de cuentas en Microsoft Office 365

- *El motor de detección de anomalías debe detectar comportamientos y acciones que parecen anormales observando en el contexto y la actividad de todos los usuarios de Microsoft Office 365.*
- *El motor de detección de anomalías debe detectar comportamientos y acciones que parecen anormales observando en el contexto y la actividad de todos los usuarios de Microsoft Office 365.*
- *Debe analizar el comportamiento, utilizando un algoritmo de aprendizaje automático, para crear un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.*
- *La solución deberá detectar anomalías del comportamiento todos los usuarios de Microsoft Office 365, tales como:*

PERÚ MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:08:02 -05:00

PERÚ MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 10:59:20 -05:00

- *Detección de comportamiento anómalo basado en motor de Inteligencia Artificial (AI) que inspecciona varios parámetros de la actividad anómala: incluyendo dirección IP, tipo de navegador, versión de navegador, dispositivo y producto VPN empleado.*
- *Geolocalización, detecta si el usuario ha iniciado sesión de sitios distantes geográficamente en un corto tiempo, inclusive desde localizaciones dentro de un mismo país.*
- *Detecta si el usuario ha iniciado sesión en un país, en el cual nunca se había iniciado sesión antes.*
- *Detecta si el usuario ha inciado sesión desde una dirección IP publica que sea categorizada como maliciosa o como fuente de envio de correos phishing.*
- *Correo electrónico inusual, detecta si el usuario tiene reglas de correos electrónicos que podrían indicar una intención maliciosa.*
- *Auto-reenvió a correo externos, cuando se crean reglas de reenvío hacia dominios externos.*
- *Fallas de autenticación de multi-factor MFA, analizando el número de eventos fallidos y satisfactorios de un usuario, para reducir la tasa de falsos-positivos.*
- *Envios masivos, detecta a través de un desvío de línea-base (baseline) a partir de un periodo de aprendizaje sobre la actividad de los usuarios internos, cuando detecta un alto volumen y genera una alerta.*
- *Anomalía de restablecimiento de contraseña, detecta cuando un usuario a recibido tres o más correos de restablecimiento de contraseña diferentes en un periodo corto de tiempo.*
- *Anomalía de eliminación de correos nuevos, detecta cuando se configura una regla de eliminación de todos los correos nuevos entrantes, para identificar robo de cuenta.*
- *Detecta cuando un usuario envia correos maliciosos de phishing al interno de la organización (destinatarios internos).*

- *La solución debe tener capacidades de análisis retrospectivo de cuentas comprometidas. Inmediatamente después de detectar una cuenta comprometida, los correos electrónicos enviados desde esta cuenta hasta 03 horas antes de la detección se deben volver a escanear con parámetros de sensibilidad más altos y, si se descubre que los correos electrónicos son maliciosos, también se deben poner en cuarentena automáticamente.*
- *Si se logró validar a través de los motores de anomalías, que la cuenta de un usuario está comprometida, la solución debe permitir tomar remediación desde la propia consola donde se registran los eventos anómalos, mediante las acciones de:*
  - *Bloquear cuenta de usuario (flujo de remediación automatizado).*
  - *Restablecimiento de la contraseña de una cuenta de usuario.*
  - *Desbloquear una cuenta de usuario bloqueada.*
  - *Restablecer contraseña y desbloquear una cuenta de usuario bloqueada.*

1.1 SOPORTE TÉCNICO

- *EL POSTOR debe contar con un Centro de Operaciones para el servicio de Soporte Técnico Local 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.*
- *El postor debe contar con un Centro de Operaciones que cumpla con las certificaciones (SOC certificado con ISO 27001 y ISO 9001) para el servicio de Soporte Técnico. Esto garantizará que se cuenten con procesos de atención óptimos que aseguren el cumplimiento de los tiempos de respuesta, la calidad de la atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y la información de la entidad. Asimismo, se asegurará la mejora continua de los procesos organizacionales y el cumplimiento de los requisitos legales y reglamentarios aplicables.*
- *La ENTIDAD podrá abrir casos directamente con el fabricante, de requerirlo, por lo que EL POSTOR deberá brindarle los accesos correspondientes.*
- *El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio de la ENTIDAD, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".*
- *El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".*
- *El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.*
- *Deberá brindar soporte técnico In Situ o remoto a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:08:12 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 10:59:29 -05:00

- *EL POSTOR deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.*
- *El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda DEL POSTOR, registrará el requerimiento y/o falla del servicio y proporcionará a la ENTIDAD un número de ticket.*

CAPACITACIÓN Y/O ENTRENAMIENTO

- *Se brindará una capacitación de 2 horas de la administración de la solución ofertada, por parte del proveedor, para dos (02) colaboradores de la Unidad Funcional de Tecnologías de la Información.*

IV. REQUISITOS DEL PROVEEDOR

2.1 Requisitos del Postor

- *Registro Único del Contribuyente (RUC) vigente, actividad económica de acuerdo al objeto de la contratación.*
- *Registro Nacional de Proveedores (RNP) vigente - bienes, de corresponder.*
- *No encontrarse inhabilitado ni suspendido para contratar con el Estado.*
- *Documento que acredite la garantía ofertada, acreditado mediante certificado de garantía, carta de garantía y/o declaración jurada.*
- *Deberá ser miembro del FIRST, lo deberá acreditar con una copia simple.*
- *Deberá contar con la ISO 27001:2022 - Gestión de la seguridad de la información.*
- *Deberá contar con la ISO 9001 - Sistemas de gestión de la calidad.*
- *Deberá contar con la ISO 37001 - Sistemas de gestión antisoborno.*
- *Experiencia mínima de tres (03) ventas relacionadas a la contratación, el mismo que debe estar acreditado con orden de compra, factura y comprobante de pago.*
- *Contar con una mesa de ayuda propia para brindar el soporte 24x7x365 incluidos domingos y feriados (Se deberá acreditar mediante declaración jurada).*
- *El postor deberá ser partner autorizado por el fabricante de la solución ofertada. Se deberá adjuntar carta del fabricante que demuestre lo requerido, (Se deberá acreditar con su respectiva carta del fabricante o distribuidor, confirmando la autorización para comercializar los productos). Lo deberá acreditar con una copia simple.*

2.2 Requisitos del Personal para la implementación

- *Un (01) Ingeniero o Técnico o Bachiller en Telecomunicaciones Redes y Comunicaciones de Datos o Computación y/o Informática o afines,*
- *El especialista en implementación de seguridad de correo electrónico y/o antispam deberá contar con experiencia no menor a un (01) año en la implementación y configuración de soluciones de protección de correo electrónico y/o antispam, el cual será acreditado con constancia y/o certificado.*
- *El especialista, deberán contar con certificación vigente por parte del fabricante en la solución a proponer.*

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:08:32 -05:00

2.3 Requisitos del Personal para el soporte

- *Un (01) Ingeniero o Técnico o Bachiller en Telecomunicaciones Redes y Comunicaciones de Datos o Computación y/o Informática o afines,*
- *El especialista en soporte de seguridad de correo electrónico y/o antispam deberá contar con experiencia no menor a un (01) año en configuración y soporte de soluciones de protección de correo electrónico y/o antispam, el cual será acreditado con constancia y/o certificado.*
- *El especialista, deberán contar con certificación vigente por parte del fabricante en la solución a proponer.*

Se podrá acreditar las certificaciones de los especialistas a cargo, presentando copias simples en idioma ginal.

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:00:28 -05:00

V. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS

NO APLICA

VI. SEGURO

NO APLICA

VII. PRESTACIONES ACCESORIAS

NO APLICA

VIII. LUGAR Y PLAZO DE ENTREGA

LUGAR:

- La licencia será entregada a través de Mesa de Partes Digital (https://mesadepartes.llamkasunperu.gob.pe/), a la Unidad de Tecnologías de la Información.

- La guía de remisión será entregada en el Almacén del Programa Llamkasun Perú, Av. Salaverry N° 655, Piso 7, Edificio del Ministerio de Trabajo y Promoción del Empleo, Jesús María.
  La entrega se efectuará previa coordinación con el responsable de Almacén o quien haga sus veces del Programa Llamkasun Perú. El horario de recepción es de lunes a viernes de 9:00 horas a 17:00 horas, teniendo en cuenta que el horario de refrigerio es de las 13:00 horas a 14:00 horas.

PLAZO: El plazo de entrega será de hasta siete (07) días calendarios, contabilizados a partir del día siguiente de la notificación de la Orden de Compra

IX. ENTREGABLES

NO APLICA

X. CONFORMIDAD

La conformidad de los bienes adquiridos será emitida por la Unidad Funcional de Tecnologías de la Información, cuyo contenido será el cumplimiento de cada punto del bien descrito.

XI. FORMA Y CONDICIONES DE PAGO

El Pago del 100% de los bienes se efectuará mediante cuenta CCI, en una armada, previa conformidad emitida por la Unidad Funcional de Tecnologías de la Información del Programa "Llamkasun Perú" con V°B° del jefe y/o quien haga sus veces.

Para efectos de pago de los bienes entregados por el contratista, la entidad deberá contar con la siguiente documentación:

- Documento de recepción de almacén (guía de remisión con recepción de almacén)
- Comprobante de pago actualizado
- Conformidad del área usuaria
- Documento que acredite la garantía ofertada
- Carta del CCI

MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:08:44 -05:00

XII. GARANTÍAS

Se establece una garantía mínima de doce (12) meses, contados a partir de la fecha de conformidad de los bienes.

El PROVEEDOR, proporcionará una garantía de doce (12) meses por el bien adquirido; dicha garantía iniciará al día siguiente de emitida la conformidad por la puesta en funcionamiento de las licencias de software antivirus.

I. CONFIDENCIALIDAD

- El Contratista se obliga a guardar reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionado con la prestación, quedando expresamente prohibido revelar dicha información a terceros. El proveedor, deberá dar

MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:00:40 -05:00

cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información.

- 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 con la prestación y/o entrega del bien y/o servicio.
- Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.
- El Contratista cederá en forma exclusiva al Programa los títulos de propiedad, derechos de autor y otro tipo de derecho de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones de la presente especificación técnica.

XIV. GASTOS POR DESPLAZAMIENTO

No aplica.

XV. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es responsable por el correcto traslado de los bienes, garantizando la integridad de los mismos.

XVI. PENALIDAD POR MORA

Penalidad por Mora en la ejecución de la prestación:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad 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

Para obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40
b) Para plazos entre sesenta y uno a ciento veinte días: F = 0.25.
c) Para plazos mayores a ciento veinte días: F = 0.15

Para consultoría de Obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40.
b) Para plazos mayores a sesenta días: F = 0.25.

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

Nota:
Asimismo, es de indicar que cualquier tipo de penalidad a aplicar puede alcanzar como máximo un monto equivalente al diez por ciento (10%) por cada entregable, del monto total del contrato vigente y/o de la orden de compra.

MTPE
Firmado digitalmente por GUZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:08:56 -05:00

VII. OTRAS PENALIDADES

No aplica.

MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:00:50 -05:00

XVIII. RESOLUCION CONTRACTUAL

Son las establecidas en el Artículo 68 de la Ley General de Contrataciones N° 32069:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

XIX. CLAUSULA ANTICORRUCION Y ANTISOBORNO

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 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.

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, participacioncitas, 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 al 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. 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. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:09:08 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:01:01 -05:00

XX. APLICACIÓN SUPLETORIA

Según Ley Nº 32069, Ley General de Contrataciones Públicas y su Reglamento, Código Civil

	Peruano, entre otras normativas vigentes.
XXI.	**MEDIDAS DE SEGURIDAD**
	No aplica.
XII.	**GESTION DE RIESGO**
	Según Literal C) del Artículo 60 de la Ley General de Contrataciones Públicas N° 32069
XIII.	**SOLUCION DE CONTROVERSIAS**
	Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y/o acción judicial.
XIV.	**CLÁUSULA DE CUMPLIMIENTO DE ACUERDO A LO ESTABLECIDO EN LA LEY N° 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".
Solicitado por:	

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Soy el autor del documento
Fecha: 12.12.2025 11:09:38 -05:00

Firma del jefe del Área Usuaria

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 12.12.2025 11:01:12 -05:00