TÉRMINOS DE REFERENCIA		
ÁREA USUARIA		UFTI – Unidad Funcional de Tecnologías de la Información
CÓDIGO Y DESCRIPCIÓN DE ACTIVIDAD - POI		C0112 – GESTION DE GOBIERNO Y TRANSFORMACION DIGITAL EN LA ENTIDAD
META PRESUPUESTARIA		004
1	DENOMINACIÓN DE LA CONTRATACIÓN	SUSCRIPCION ANUAL A LICENCIA DE SOFTWARE ANTIVIRUS
2	FINALIDAD PÚBLICA, ALCANCE Y DESCRIPCIÓN DEL SERVICIO	**2.1 Finalidad pública** Garantizar la seguridad, integridad y disponibilidad de la información institucional del Centro Nacional de Planeamiento Estratégico – Ceplan, mediante la suscripción anual a licencias de software antivirus, que permitan fortalecer la protección de los equipos de cómputo y de la infraestructura tecnológica institucional frente a amenazas informáticas. **2.2 Antecedente** El Centro Nacional de Planeamiento Estratégico – Ceplan cuenta con equipos de cómputo y plataformas tecnológicas que soportan el procesamiento, almacenamiento y provisión de servicios institucionales, los cuales requieren protección permanente frente a amenazas informáticas tales como virus, malware, ransomware y otros tipos de ataques cibernéticos. Mediante la Resolución de Dirección Ejecutiva N.° 005-2025/CEPLAN/DE, de fecha 18 de diciembre de 2025, se aprobó la compatibilización del Requerimiento de Software Antivirus, estableciéndose un período de vigencia de cinco (05) años. En cumplimiento de las políticas de seguridad de la información y de las directivas emitidas por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros (PCM), el Ceplan mantiene implementadas soluciones de software antivirus orientadas a garantizar la integridad, disponibilidad y confidencialidad de la información institucional. **2.3 Objetivos de la contratación** **2.3.1 Objetivo general:** Garantizar la protección integral del entorno tecnológico del Ceplan mediante la suscripción anual a licencias de software antivirus SOPHOS CENTRAL INTERCEPT X ADVANCED, asegurando la continuidad operativa, la integridad de la información y la reducción de riesgos cibernéticos. **2.3.2 Objetivos específicos:** • Asegurar la protección continua y actualizada de todos los activos tecnológicos institucionales. • Prevenir y mitigar amenazas informáticas tales como virus, malware, ransomware y otros ataques cibernéticos. • Contar con una plataforma centralizada de administración y monitoreo que permita la gestión eficiente de la seguridad informática. • Cumplir con las políticas de seguridad de la información y de gobierno digital establecidas por la Presidencia del Consejo de Ministros (PCM). • Garantizar la disponibilidad, confidencialidad e integridad de la información institucional, contribuyendo al adecuado funcionamiento de los sistemas del Ceplan. **2.4 Alcances y descripción del servicio** **2.4.1 Alcances:** El presente servicio comprende la suscripción anual a licencias de software antivirus, destinadas a la protección integral de los dispositivos y plataformas tecnológicas institucionales del Ceplan que soportan el procesamiento, almacenamiento y provisión de servicios de información. El alcance incluye la activación, configuración y soporte técnico de las licencias durante un periodo de un (1) año, garantizando la cobertura total de los activos tecnológicos institucionales, la actualización continua de los mecanismos de protección y la administración centralizada de la seguridad informática. **2.4.2 Descripción del servicio:** La entidad contrata el servicio de suscripción anual de licencias de software antivirus de un solo fabricante, que incluya consola de administración y agentes de protección, orientado a la protección de los equipos de cómputo y plataformas tecnológicas institucionales del Ceplan. El proveedor deberá suministrar, activar, habilitar y mantener licencias de software antivirus SOPHOS CENTRAL

INTERCEPT X ADVANCED, garantizando su operatividad continua durante el período contratado, bajo un esquema de administración centralizada.

El servicio se prestará conforme al siguiente detalle:

EQUIPAMIENTO	DESCRIPCION	CANTIDAD	TIEMPO
EQUIPOS DE CÓMPUTO Y PLATAFORMAS TECNOLÓGICAS	CENTRAL INTERCEPT X ADVANCED	200	365 días (1 año)

2.4.3 Características del servicio

El software antivirus debe ofrecer protección integral de sistemas operativos y plataformas tecnológicas institucionales, con capacidades de defensa avanzada, administración centralizada y soporte continuo.

a) Protección para computadoras de escritorio y computadora portátil personal

- 120 equipos con Windows 10 y 11 (64 bits).
- Detección en tiempo real, bloqueo de malware, ransomware y amenazas de día cero.
- Uso de inteligencia artificial y análisis de comportamiento.
- Protección web y escaneo HTTPS, firewall personal, y control de intrusiones.
- Administración centralizada mediante agente, políticas de escaneo, contraseñas de protección y exclusiones configurables.

b) Protección para plataformas tecnológicas institucionales

- 80 equipos con Windows Server (2016, 2019) y Linux.
- Protección en tiempo real, con autodefensa ante ataques y exclusiones automáticas.
- Herramientas forenses para análisis de incidentes.
- Capacidad de lista blanca y monitoreo de archivos críticos del sistema.

c) **Protección contra amenazas avanzadas**

- Uso de machine learning y deep learning para detección sin firmas.
- Protección AMSI contra scripts maliciosos.
- Bloqueo proactivo de ransomware, spyware, troyanos y cryptominers.
- Análisis forense y registro detallado de conexiones, procesos y eventos.
- Prevención de intrusiones, escalamiento de privilegios e inyección de código.

d) **Protección contra ransomware**

- Protección basada en comportamiento y no solo en firmas.
- Capacidad de remediación de archivos cifrados.
- Reporte de incidentes y análisis de causa raíz desde la consola.
- Prevención de cifrado remoto y bloqueo del origen del ataque.

e) **Protección contra vulnerabilidades**

- Bloqueo de exploits, robo de credenciales y escalamiento de privilegios.
- Mitigación de inyecciones de código y migración de procesos maliciosos.

f) **Consola de administración**

- Administración centralizada vía web o nube, con panel de control y alertas.
- Roles de usuario, sincronización con Active Directory, políticas por grupo y actualizaciones automáticas.
- Reportes exportables (CSV, PDF), monitoreo detallado y alertas por correo.
- Control de ancho de banda, aislamiento de equipos, y actualizaciones graduales.
- Integración con servidores en la nube (ej. AWS).
- Módulos adicionales
- Control de aplicaciones: restringe la ejecución de software no autorizado.
- Control web: filtra sitios por categorías y horarios, con listas blancas y negras.
- Control de periféricos: gestiona permisos de USB y otros dispositivos.
- Detección y respuesta (EDR/XDR)
- Identificación y análisis de amenazas mediante marco MITRE ATT&CK.
- Investigación guiada y búsqueda proactiva de indicadores de compromiso.
- Aislamiento automático o manual de equipos comprometidos.
- Consultas forenses, almacenamiento histórico (90 días) y módulo de inteligencia artificial para threat hunting.

g) Protección para plataformas tecnológicas institucionales

- Proteger en tiempo real contra códigos maliciosos, ransomware y amenazas de día cero.
- Utilizar inteligencia artificial y aprendizaje profundo para detectar y eliminar amenazas.
- Evitar la modificación o detención de procesos críticos del sistema.
- Mantener la protección activa desde el inicio del sistema operativo.
- Permitir exclusiones, escaneos manuales y programados.
- Integrarse a una consola central (en nube o local) para administración.
- Generar reportes automáticos del estado de protección.
- Incluir firewall y mecanismos IPS/IDS contra ataques de red.
- Monitorear el comportamiento de procesos del sistema.
- Brindar protección tanto para entornos físicos como virtualizados.

h) Protección contra amenazas avanzadas

- Detectar amenazas mediante análisis de comportamiento e inteligencia artificial.
- Bloquear ataques en memoria, robo de credenciales y escalamiento de privilegios.
- Impedir la ejecución de troyanos, gusanos, keyloggers y cryptominers.
- Detectar y neutralizar scripts maliciosos y amenazas emergentes.
- Permitir el aislamiento del componente comprometido.
- Incluir funciones forenses y de registro de eventos críticos.
- Integrar detección y respuesta avanzada (EDR/XDR).

i) Protección contra ransomware

- Implementar defensa basada en comportamiento, sin depender de firmas.
- Detectar y revertir intentos de cifrado de archivos.
- Notificar incidentes con detalles del ataque.
- Prevenir cifrado remoto desde otros equipos conectados.
- Mantener copias seguras para restauración automática.

j) Protección contra vulnerabilidades y técnicas de explotación

- Proteger frente a exploits y vulnerabilidades conocidas o no.
- Bloquear la inyección de código en procesos legítimos.
- Impedir manipulación del registro y acceso no autorizado a memoria.
- Detectar escalamiento de privilegios o cambios de permisos.
- Monitorear y bloquear actividades anómalas en procesos críticos.

k) Consola de administración

- Ser centralizada, web (nube o local), y administrar servidores y endpoints.
- Mostrar paneles con estado de protección y alertas.
- Permitir políticas diferenciadas por grupos o dispositivos.
- Sincronizar con Active Directory.
- Permitir despliegue remoto o manual (GPO).
- Actualizar automáticamente motores y definiciones.
- Generar reportes automáticos (CSV, PDF).
- Configurar escaneos, exclusiones y firewall.
- Comunicarse mediante HTTPS y enviar alertas por correo.
- Mostrar información del servidor y análisis de causa raíz.
- Incluir mapas de amenazas y capacidades de búsqueda proactiva (MITRE ATT&CK).

l) Control de aplicaciones, web y periféricos

- Controlar la ejecución de aplicaciones no autorizadas.
- Aplicar restricciones por tipo o categoría.
- Gestionar acceso web por listas blancas y negras.
- Definir políticas por horario o grupo.
- Monitorear y restringir el uso de periféricos (USB, discos externos, Bluetooth, etc.).
- Establecer permisos según tipo de dispositivo (lectura, escritura, bloqueo).

2.4.4 INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO

El contratista deberá de realizar la implementación, configuración y funcionamiento del software antivirus, considerando por ello lo siguiente:

- Los trabajos programados serán supervisados por el personal de la Unidad Funcional de Tecnología de Información.
- Instalación de la herramienta para la sede del Ceplan
- Instalación de la consola principal, además de subconsolas de ser el caso, las cuales serán determinadas

por la Unidad Funcional de Tecnología de Información.

- Instalación y configuración del software de antivirus en las estaciones de trabajo de la entidad, ubicados en la Sede Principal.
- Toda la solución debe estar basada únicamente en software, la solución no deberá incluir la adquisición de ningún tipo de equipamiento adicional como complemento de este.
- El software no debe afectar lentitud en los equipos de cómputo conectados a la Red del Ceplan.

Asimismo, el software antivirus a adquirir deberá contar como mínimo las siguientes características técnicas:

2.4.5 SOPORTE TÉCNICO

a) Soporte y actualización de licencias antivirus por el periodo de ejecución del servicio.
b) El contratista deberá contar con soporte técnico disponible de lunes a viernes, de 8:30 a.m. a 6:00 p.m., y los sábados, de 9:30 a.m. a 12:00 p.m., durante los 365 días del año. Asimismo, deberá disponer de la posibilidad de escalar casos técnicos en cualquier momento a la casa matriz, haciendo uso del sistema del fabricante.
c) El contratista brindará los datos como números telefónicos y correos electrónicos para las coordinaciones y comunicación con la Entidad.
d) Si en caso la llamada realizada por el personal de soporte técnico no tuviera éxito en contactarse, se procederá a enviar un correo electrónico que deberá asignar el contratista para la atención inmediata, una vez realizado él envió el contratista tendrá que devolver la llamada en un tiempo máximo de 180 minutos.
e) Si se presenta cualquier incidencia o vulnerabilidad en la red de la solución de seguridad del contrato, el área usuaria reportará la incidencia a través de correo electrónico y el contratista tendrá un tiempo de respuesta de 04 horas como máximo desde reportada la incidencia, para dar solución a la incidencia reportada.
f) El proveedor podrá brindar el soporte de forma remota, para lo cual se le brindará el acceso respectivo para evaluar la incidencia y atenderla. Luego de atendida la incidencia, el proveedor deberá remitir un correo electrónico indicando la culminación de la atención.
g) En caso la incidencia no pueda ser atendida de forma remota, el proveedor asignará un técnico el cual se apersonará a las instalaciones de la Entidad, dentro de las 24 horas siguientes de ser reportada la incidencia.

2.4.6 CAPACITACION

a) Mínimo 6 horas de capacitación sobre administración y configuración del antivirus.
b) Dirigida a tres personas, de forma virtual o presencial, posterior a la implementación
c) El contenido de la capacitación deberá desarrollar como mínimo los siguientes temas:
   - Instalación
   - Configuración
   - Administración
   - Solución de problemas sobre los componentes de la herramienta
   - Durante el curso de capacitación el oferente deberá realizar pruebas de ataques reales, infectando una máquina de prueba
   - Despliegue de políticas de seguridad de las consolas y sub consolas instaladas en la red del Ceplan
d) Al finalizar la capacitación, el contratista deberá otorgar certificados de Operador y Administrador de Consola del producto adquirido a los participantes.

2.5 Otras Consideraciones

No aplica

2.6 Facilidades a ser provistos por la Entidad

Para la adecuada ejecución del servicio, el Ceplan se compromete a brindar al CONTRATISTA las siguientes facilidades, las cuales no generan vínculo laboral ni dependencia alguna:

a) Otorgar facilidades razonables de acceso a las instalaciones de la institución, de manera excepcional y únicamente cuando resulte indispensable para la entrega o validación de los productos del servicio, previa coordinación puntual y autorización del jefe inmediato del área usuaria, sin que ello implique sujeción a jornada, horario regular, permanencia continua, asignación de puesto de trabajo ni supervisión funcional.
b) Proporcionar la información y documentación necesaria, estrictamente vinculada al objeto del servicio, como insumo para la elaboración de los entregables contratados. Dicha entrega no supone transferencia de funciones, responsabilidad operativa, dirección funcional, ni habilitación para ejecutar actividades propias del personal de la entidad.
c) El contratista deberá garantizar la operatividad de los servicios ininterrumpido durante el período de inicio de la implementación.
d) Cualquier solicitud posterior de reconfiguración del servidor donde se instalará la consola de antivirus, deberá realizarse sin costo adicional para CEPLAN. El software de antivirus provisto por el contratista debe cumplir con las características técnicas propuestas.

2.7. Desplazamientos para el desarrollo del servicio:

No aplica

3	RESULTADO ESPERADO	**Entregable Único.** • Documento que acredite la suscripción activa y vigente de las licencias Sophos Central Intercept X Advanced durante el periodo contratado. • Reportes del sistema que acrediten la protección en tiempo real contra malware, ransomware, exploits y ataques de día cero. • Evidencia documental que demuestre la administración unificada de las licencias mediante una consola (en nube o local), permitiendo la gestión, supervisión y generación de reportes del estado de protección de todos los activos tecnológicos institucionales. La actualización automática de motores de detección, definiciones y módulos de seguridad. • Documento de compromiso y evidencia de acceso a soporte técnico especializado durante la vigencia de la suscripción. • Documento que acredite la ejecución de la capacitación técnica brindada al personal designado para la correcta gestión y operación de la plataforma antivirus. • Documento que detalle el contenido de la capacitación realizada y el compromiso del soporte técnico, indicando número telefónico y correo electrónico exclusivo de atención. • Documento que acredite la suscripción activa y vigente de las cuentas Sophos Central Intercept X Advanced durante el periodo contratado. • Acta de activación de las cuentas, debidamente firmada entre el proveedor y el área usuaria, que certifique el inicio del servicio. El proveedor deberá entregar vía electrónica a la mesadepartesvirtual@ceplan.gob.pe los documentos correspondientes.
4	REQUERIMIENTO DEL PROVEEDOR Y DE SU PERSONAL	**DEL PROVEEDOR** **4.1 Requisitos del proveedor** • Persona natural y/o jurídica • Tener RUC activo y habido. • No encontrarse inhabilitado, impedido o sancionado para contratar con el Estado. • Encontrarse inscrito en el Registro Nacional de Proveedores (RNP), de corresponder. • El proveedor debe ser partner certificado de la marca a cotizar en la categoría Platinium en adelante, lo cual deberá acreditar con certificado, constancia o carta emitida por el fabricante de la marca, la misma que deberá ser presentada previo a la suscripción del contrato. • El proveedor debe de contar con un sistema de tickets. Enviar evidencia. • El proveedor debe de contar con un área de Helpdesk. **4.2. Perfil del proveedor** El proveedor debe acreditar un monto facturado acumulado equivalente S/ 40,000.00 (cuarenta mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. **Acreditación**: La experiencia requerida se acreditará de la siguiente forma: (i) copia simple de contratos (ii) constancias de trabajo o (iii) constancias de prestación de prestación de servicio o cualquier otra documentación que de manera fehaciente acredita la experiencia. **Nota**: Los documentos presentados en un idioma diferente al español deberán estar con la respectiva traducción por traductor público juramentado o traductor colegiado certificado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que puede ser presentada en el idioma original
5	CONDICIONES DE CONTRATACIÓN	**5.1 Modalidad de pago** El contrato se rige por la modalidad de suma alzada. **5.2 Seguros aplicables:** No aplica **5.3 Garantías** De conformidad con el artículo 60 de la Ley N.º 32069 y el artículo 227 del Reglamento, para la presente contratación menor, no se exigirá garantía de fiel cumplimiento.

		5.4 Gestión de Riesgo Las PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato/orden de servicio u compra 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.
6	LUGAR Y PLAZO DEEJECUCIÓN	**6.1 Lugar:** El servicio será prestado de forma remota/virtual, a través de medios digitales de comunicación, coordinación y entrega, habilitados por el proveedor y/o por la entidad contratante. El contratista deberá garantizar la disponibilidad de los recursos tecnológicos necesarios para la ejecución eficiente de las actividades encomendadas. La modalidad virtual no exime al contratista del cumplimiento de los plazos, entregables, calidad y demás condiciones establecidas en los presentes Términos de Referencia, ni de la obligación de atender coordinaciones presenciales cuando la entidad lo requiera de manera justificada. Para las actividades que se lleven a cabo de manera presencial, estas se realizarán en las instalaciones del Ceplan (Av. Canaval y Moreyra N.º 480 piso 21 o Auditorio piso 2, de corresponder – San Isidro), previa coordinación con el área usuaria. **6.2 Plazo:** El plazo de ejecución del servicio será de la siguiente manera: 1. Para la activación de la suscripción: El plazo será de 5 días, computado a partir del día siguiente de notificada la orden de servicio. 2. Plazo de vigencia del servicio será de 365 días calendario contados a partir del día de la activación de la suscripción, el cual se suscribirá un acta de inicio suscrito por el área usuaria y el proveedor, de acuerdo a la necesidad del área usuaria.
7	MEDIDAS DE CONTROL	**7.1 Áreas que supervisan:** Unidad Funcional de Tecnologías de la Información. **7.2 Áreas que coordinarán con el proveedor:** Unidad Funcional de Tecnologías de la Información. **7.3 Área que brindará la conformidad:** será otorgada por la Unidad Funcional de Tecnología de la Información de la Oficina General de Administración. **Nota:** La conformidad debe emitirse en un plazo máximo de siete (7) días contabilizados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, o si se trata de consultorías, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad del servidor o funcionario que debe emitir la conformidad. La sola recepción de bienes en la entidad o en el destino final, según sea el caso, no constituye la conformidad del área usuaria. De conformidad al artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.
8	FORMA Y CONDICIONES DE PAGO	Como retribución de los servicios prestado, el Ceplan deberá realizar el pago de la contraprestación pactada a favor del CONTRATISTA, en Soles incluido impuestos de Ley, según la cotización, pagadero en UNA (1) armada siendo el 100% del monto de la contratación. El pago de la retribución se realizará previa conformidad, siempre que el CONTRATISTA haya cumplido con entregar los resultados esperados. EL CONTRATISTA deberá adjuntar lo siguiente: - Carta simple dirigida al Ceplan, precisando en su contenido, el número de contrato y/o orden de servicio, objeto de EL SERVICIO. - Acta de la activación de las cuentas firmada entre el proveedor y el área usuaria. - Comprobante de pago El pago se realizará a través del Código de Cuenta Interbancaria del proveedor, CONTRA PRESENTACIÓN Y APROBACIÓN del entregable.
9	PRESENTACIÓN Y RECEPCIÓN DEL PRODUCTO/ENTREGABLE	La presentación del (los) entregable(s) podrá realizarse a través de la Mesa de Partes Virtual, mediante el envío al correo electrónico **mesadepartesvirtual@ceplan.gob.pe** , dirigido al CEPLAN, con copia a la Unidad Funcional de Tecnología de la Información; o, de manera alternativa, a través de la Mesa de Partes Presencial, ubicada en la Av. Canaval y Moreyra N.º 480, piso 21 – San Isidro, dentro del horario vigente de recepción de documentos. Los entregables (documentos) deberán encontrarse debidamente firmados, ya sea de manera manuscrita o electrónica. En el caso de que el entregable sea suscrito con firma digital (RENIEC), será suficiente la consignación de una sola firma. Si el día de entrega del producto/entregable establecido en los presentes Términos de Referencia, coincide con un día no laborable, se correrá la fecha de entrega hasta el siguiente primer día hábil, sin que sea sujeto de penalidad **OBSERVACIONES AL ENTREGABLE/PRODUCTO:** De existir observaciones, la Dependencia Encargada de las Contrataciones comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar dependiendo de la complejidad o sofisticación de las subsanaciones a realizar.

		El plazo de subsanación no será mayor del 30% del plazo del entregable correspondiente. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.
10	PENALIDAD	**0.1 Penalidad por Mora:** Se aplicará penalidad por mora, conforme al siguiente detalle: 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: $$Penalidad\ diaria = \frac{0.10 \times monto}{F \times plazo}$$ Donde F tiene los siguientes valores: Para bienes y servicios: F = 0.40 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. **10.2 Otras Penalidades:** No aplica **Nota:** La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente. La entidad contratante considera las particularidades de las otras penalidades.
11	OTROS ASPECTOS	**11.1 Confidencialidad:** El profesional a contratar deberá guardar reserva de toda la información de carácter administrativa, organizativa, técnica entre otros, a que tenga acceso en virtud de los servicios que prestará. **11.2 Responsabilidad por Vicios Ocultos:** El contratista tiene un plazo máximo de un año por responsabilidad por la calidad ofrecida y por los vicios ocultos de los servicios ofertados. **11.3 Resolución Contractual:** Cualquiera de las partes podrá resolver, total o parcialmente, la Orden de Servicio o Contrato, conforme a lo establecido en el numeral 68.1 del artículo 68 de la Ley N.º 32069 – Ley General de Contrataciones Públicas. En caso la resolución total o parcial de la orden de servicio y/o contrato sea promovida por la Entidad, esta deberá contar con un informe sustentatorio emitido por el área usuaria. Con dicho sustento, se remitirá la respectiva Resolución Jefatural, la cual será notificada al contratista por correo electrónico. Posteriormente, se dará inicio al procedimiento de pago correspondiente a la parte ejecutada del servicio, deduciendo los gastos incurridos y aplicando las penalidades que correspondan, siempre en base al informe de conformidad emitido por el área usuaria. Si la resolución es solicitada por el contratista, este deberá presentar una carta formal exponiendo los motivos de su decisión de resolución total o parcial del servicio contratado. El Área Usuaria emitirá un informe donde acepte o deniegue la propuesta; de ser aceptada procederá a efectuar el cálculo del servicio efectuado. Con ello, la Unidad Funcional de Abastecimiento determina el procedimiento de pago de la proporción ejecutada, considerando la aplicación de penalidades y gastos que correspondan, y comunicará al proveedor la aceptación de la solicitud, adjuntando resolución. **Nota:** Por la implementación progresiva de la Plataforma Digital para las Contrataciones Públicas (PLADICOP), las notificaciones durante la ejecución del contrato se realizarán al correo electrónico previsto en el contrato y/o orden de servicio y surten efectos desde su recepción. **11.4 Clausula de Anticorrupción y Antisoborno:** EL PROVEEDOR declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato. Asimismo, EL PROVEEDOR se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores. Además, EL PROVEEDOR debe comunicar a las autoridades competentes,

		de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas https://denuncias.servicios.gob.pe/ **11.5 Solución de Controversias:** Todas las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia, se resuelven mediante conciliación, conforme lo dispuesto en el numeral 81.3 del artículo 81 de la Ley 32069. El procedimiento conciliatorio será regulado mediante el numeral 330.2 del artículo 330 del Reglamento.

Firmado digitalmente por ROJAS VASQUEZ Carlos Alberto FAU 20520594451 soft Motivo: Soy el autor del documento Fecha: 10.02.2026 11:37:19 -05:00	Firmado digitalmente por MAGUIÑA ROCA Edgar Williams FAU 20520594451 soft Motivo: Doy V° B° Fecha: 10.02.2026 16:11:38 -05:00
FIRMA	FIRMA