CONTRATO MENOR
ESPECIFICACIONES TECNICAS

1. ÁREA USUARIA Y/O ÁREA TÉCNICA ESTRATÉGICA:

Oficina de Sistemas

2. DENOMINACION DE LA CONTRATACION:

Adquisición de Software y Licencias de Antivirus para el Organismo de Formalización de la Propiedad Informal – COFOPRI

3. FINALIDAD PÚBLICA:

El presente proceso permitirá proteger nuestros equipos y servidores frente a las amenazas digitales. El antivirus actualizado ayuda a prevenir virus y proteger nuestra información personal y de los ciudadanos realizando trabajos de escaneos frecuentes y evitar descargar archivos de fuentes no confiables.

4. OBJETO DE LA CONTRATACION:

Adquirir el software y las licencias de antivirus necesarias para garantizar la protección de los sistemas informáticos del Organismo de Formalización de la Propiedad Informal (COFOPRI), esto permitirá proteger la infraestructura tecnológica de amenazas digitales, prevenir posibles ataques informáticos, salvaguardar la información confidencial y asegurar la continuidad de las operaciones administrativas y operativas, contribuyendo así a la eficiencia y seguridad de la entidad en el desempeño de sus funciones.

5. ACTIVIDAD DEL POI:

- **Actividad Presupuestal:** Gestión Administrativa
- **Actividad Operativa:** C0091 “Atencion de la Continuidad y Operatividad al Data Center”
- **Secuencia Funcional:** 125

6. DESCRIPCION DEL/LOS BIEN(ES):

La presente adquisición comprende lo siguiente:

ITEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN
1	1400	Unidad	Software (Inc. Licencia) antivirus corporativo

6.1 CARACTERÍSTICAS Y CONDICIONES DE LA CONTRATACIÓN

COMPATIBILIDAD

- Microsoft Windows 7 Sp1 y superior
- Microsoft Window Server 2008 R2 y superior
- MacOS 10.12 o superior
- Linux Ubuntu 14.04 LTS o superior, Fedora 23 o superior, Debian 8 o superior, CentOS 6.2 o superior, Alma Linux 8.4 o superior, Linux Mint 18 o superior, SUSe Linux Enterprise 11 SP2 o superior, Oracle Linux 6.5 o superior, Open Suse 15.5 o superior.
- Android 10 o superior.
- iOS 13 o superior.

CONSOLA DE ADMINISTRACIÓN

- Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo y dispositivos móviles deben ser suministrados por un solo fabricante, NO SE ACEPTARÁN COMPOSICIONES DE PRODUCTOS DE DIFERENTES FABRICANTES.
- La consola de administración debe ser accedida mediante un usuario, contraseña y autenticación multifactor (MFA) para garantizar una mayor seguridad
- La solución debe clasificarse como EDR (Endpoint Detection and Response).
- Esta solución debe incluir antimalware, EDR, Filtro Web, Control de dispositivos periféricos, firewall, sistema de prevención de intrusos, control de aplicaciones.
- La consola de monitoreo y configuración deberá ser a través de una central única basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos ofertados.
- La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional.
- El agente del producto debe ser capaz de escanear la red en búsqueda de máquinas desprotegidas.
- Debe poseer un mecanismo de comunicación, para su integración, con otras soluciones de seguridad
- La solución debe permitir identificar y visualizar las técnicas y tácticas utilizadas en un intento de ataque para facilitar la respuesta a incidentes.
- La consola de administración debe permitir la administración de los equipos ya sea a través de grupos o mediante la asignación directa de políticas a determinadas máquinas. Debe ser también posible crear subgrupos con políticas distintas a los grupos padres, siendo necesario anidar grupos hasta al menos 4 niveles.
- La consola de administración al igual que los clientes debe estar al menos en idiomas inglés y español.
- Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección
- La instalación debe poder realizarse a través del cliente descargado de la consola central, vía correo electrónico y desde la propia consola nube usando una maquina con métodos de despliegue remoto masivo y distribución local de paquetes para optimizar el ancho de banda que permite la distribución de los paquetes de instalación del antivirus.

- Proporcionar actualizaciones del producto y de las definiciones de malware, phishing, aplicaciones y protección contra intrusos durante el tiempo de licenciamiento del producto.
- Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso; tanto a nivel global, como específico en cada política
- La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros.
- Permitir la programación de la exploración contra malware con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
- Utilizar protocolos seguros estándar HTTPS/TLS para la comunicación entre la consola de administración y los clientes administrados.
- Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
- Permitir la exportación de los informes gerenciales en los formatos PDF, XLSX o CSV.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
- Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
- Capacidad de generación de informes, estadísticas o gráficos, tales como:
  - Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
  - Detalle de las versiones del antivirus que están instalados en los equipos
  - Equipos que requieren reinicio.
- La solución deberá permitir una prueba de actualización sobre un grupo de equipos piloto antes de implementarlo para toda la red. También debe permitir seleccionar un grupo de equipos que se encarguen de la actualización de firmas/conocimiento y del propio producto (caché) para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales. Estos servidores caché deben ser configurados para que atiendan a determinado grupo de equipos o a múltiples grupos.
- La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo, servidores, celulares con sistemas operativos Windows, Linux, mac, Android y iOS y debe diseñarse para administrar, supervisar y elaborar informes de dispositivos, endpoint y servidores.
- La Consola de administración debe incluir un panel con un resumen visual para comprobar el estado de seguridad en las últimas 24 horas y en el último mes.
- Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención. Estos filtros también deberán poder ser personalizados por el administrador de la herramienta.
- Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría:
  - Detalles del estado del equipo
  - Detalles sobre la actualización
  - Detalles de avisos y errores
  - Usuario logueado en la maquina

- Dirección ip de la máquina
- Dominio
- Ruta del directorio activo donde pertenece la máquina.
- Detalles del antivirus, etc. y ordenar los equipos en consecuencia

- La consola de administración nube, debe permitir al administrador al menos realizar las siguientes acciones:
  - Inicio de un escaneo en la máquina en búsqueda de malware.
  - Forzar una actualización de definiciones de malware.
  - Ver los detalles de los eventos ocurridos.
  - Forzar el cumplimiento de una nueva política de seguridad.
  - Mover el equipo a otro grupo.
  - Borrar el equipo de la lista.
  - Desinstalación del antimalware y del agente en la maquina
  - Aislar la máquina.
  - Reiniciar la máquina.
  - Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro manual o automáticamente.
- Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses.
- Deberá permitir exportar el informe de registros de auditoría al menos en formato CSV
- Ante un evento de infección o de ataque consecutivo la consola debe ser capaz de aislar el equipo para evitar la propagación de la infección.
- Debe contener varios informes para el análisis y control de los usuarios y endpoint. Los informes se deben dividir, en informes de: eventos de malware, control de aplicaciones, periféricos, web, indicadores de ataque, máquinas sin parchar o con falta de parches críticos, ataques de red, actividades de xploits, estado de protección de las maquinas, indicando todas las funciones solicitadas para los endpoint.
- Deberá tener la posibilidad de instalar un servidor para reenvío de eventos y políticas de seguridad (relay/proxy) en caso de que el agente no pueda comunicarse con la consola en la nube.
- Deberá tener la posibilidad de implementar servidores de caché locales para la descarga de parches y actualizaciones de sistema operativo, aplicaciones y malware, para de esta manera tener un uso eficiente del ancho de banda. Esta máquina caché podrá ser cualquier máquina que tenga el agente instalado sin necesidad de recurrir a un appliance virtual o algún equipo adicional dedicado para tal fin.
- El agente del producto debe ser capaz de desinstalar otras soluciones antimalware instaladas previamente en los equipos cliente.
- Desde la consola de administración debe ser posible hacer un inventario de software que puede ser exportado al menos en CSV donde muestre todos los productos instalados en los equipos, pudiendo obtener esta información de manera global o de un equipo especifico.
- Para que se puede medir el performance de los equipos, desde la consola de administración debe poder observarse el consumo de al menos cpu, memoria y disco duro durante las últimas 24 horas.
- El producto debe ser capaz de evaluar las vulnerabilidades de los sistemas operativos (Windows, Linux, Mac), pudiendo indicar que parches de seguridad ya sea de aplicaciones o de sistema operativo faltan en los equipos y los niveles de peligrosidad asociados a estas vulnerabilidades. Estas vulnerabilidades deben indicar el CVE asociado.

- La consola de administración debe ser capaz de poner en modo auditoría a los agentes de antimalware, para permitir la convivencia inicial con otras soluciones antimalware de ser necesario. En el modo auditoría el producto detectará malware y otros tipos de ataques, pero solo notificará y no tomará acción.
- La consola de administración debe permitir la eliminación automática de aquellos equipos que no se conectan por cierta cantidad de tiempo determinada por el administrador.
- Desde la consola de administración el administrador de la herramienta debe ser capaz de retirar la licencia o asignársela a una máquina. Así como la eliminación del antimalware y el agente de manera remota.
- Desde la consola el administrador de la herramienta puede mandar a comparar el hash del nuevo malware con Virus Total para hacer un descarte inicial.

AGENTE DE PROTECCIÓN CONTRA MALWARE:

- Capacidad de eliminación automática de spyware, adware, gusanos, virus, ransomware y PUAs.
- La solución debe permitir enviar archivos con posibles amenazas al centro de operaciones del fabricante para su análisis y una conexión directa para la retroalimentación de información.
- El agente instalado en los dispositivos no debe depender de la nube para la función de detección y respuesta ante amenazas (autónomo). Debe ser capaz de operar eficazmente tanto en línea como fuera de línea.
- Debe ofrecer detección y respuesta en tiempo real a eventos que ocurren en puntos finales, incluidos scripts maliciosos, ejecución PE anormal, malware sin archivos (fileless), exploits de aplicaciones y sistemas operativos, actividades de proceso anormales, scrapes de memoria y credenciales, shells inversos, exploits de día cero, ataques a memoria
- Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
- Debe realizar la verificación de todos los archivos accedidos en tiempo real.
- Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUAs)
- Deberá detectar malware y phishing durante la navegación web.
- Debe permitir la autorización de aplicaciones desconocidas y excluirlas de la exploración de directorios y archivos específicos.
- Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas.
- Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
- Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de la protección.
- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida
- Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.

- Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
- El producto debe ser capaz de integrarse con AMSI.

DETECCIÓN PROACTIVA DE RECONOCIMIENTO DE NUEVAS AMENAZAS

- Protección contra amenazas de día zero a través de tecnología de Machine learning.
- Protección contra exploits.
- Protección contra amenazas avanzadas persistentes (APT).
- Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Machine learning.
- Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
- No debe requerir descarga de firmas de ningún tipo.
- Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
- Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro. Este análisis de causa raíz debe mostrar de forma detallada la cadena de eventos, incluyendo procesos, sub-procesos ejecutados y modificaciones en el sistema.
- Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas.
- El producto debe contar con tecnología sandboxing tanto local como en nube para la evaluación y detección de nuevo tipo de malware.
- El producto debe contar con protección de amenazas de día zero, mediante el bloqueo de aplicaciones y complementos desconocidos hasta que el sandboxing local y/o remoto den un veredicto.
- El producto debe ser capaz de monitorear de manera gráfica en los equipos protegidos puertos determinados indicados por el administrador y la interacción de otros equipos protegidos o sin proteger con estos puertos.
- Generación de excepciones ante falsos positivos.

PROTECCIÓN CONTRA VULNERABILIDADES Y TÉCNICAS DE EXPLOTACIÓN

- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero;
- Detección y protección de las siguientes técnicas de explotación:
  - Enforce Data Execution Prevention;
  - Mandatory Address Space Layout Randomization;
  - Bottom-up ASLR;
  - Null Page (Null Deference Protection);
  - Heap Spray Allocation;
  - Dynamic Heap Spray;
  - Stack Pivot;
  - Stack Exec (MemProt);
  - Stack-based ROP Mitigations (Caller);
  - Branch-based ROP Mitigations (Hardware Assisted);
  - Structured Exception Handler Overwrite (SEHOP);
  - Import Address Table Filtering (IAF);
  - Load Library;
  - Reflective DLL Injection;

- Shellcode;
- VBScript God Mode;
- Wow64;
- Syscall;
- Hollow Process;
- DLL Hijacking;
- Squiblydoo Applocker Bypass;
- APC Protection (Double Pulsar / AtomBombing);
- Process Privilege Escalation

- Mitigación de inyección de códigos en procesos.
- Protección contra malware oculto en aplicaciones legítimas (code cave).
- Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
- Evitar obtener escalada de privilegios y acceso elevado a recursos.
- Modificación de claves de registro para la ejecución de código arbitrario.

COMPONENTES DE SEGURIDAD ADICIONALES:

- Además del control de amenazas, el mismo agente debe proporcionar control de dispositivos, control de aplicaciones, control web, IPs, firewall y filtro web por categorías
- El producto debe permitir habilitar y deshabilitar dispositivos periféricos como:
  - Medios removibles
  - Lectores de CD/DVD
  - Dispositivos bluetooth.
  - Dispositivos móviles
  - módems
- El producto debe contar con un firewall, permitiendo crear reglas por puertos y aplicaciones específicas, pudiendo el firewall especificar cosas como el sentido de la comunicación, puertos y la acción a tomar
- El producto debe contar con una herramienta de filtro web basado en categorías, debiendo contar al menos con 60 categorías web, dentro de las cuales deben incluirse: juegos de azar, juegos, material adulto, internet radio y TV, P2P, sitios multimedia, sitios de Inteligencia Artificial, compras, redes sociales, youtube, entre otros.
- La política de filtro web debe poder personalizarse para que funcione en un horario especifico y en determinados días de la semana.
- El producto debe contar con un sistema de prevención de intrusos (IPS) para protección contra ataques de red.
- Debe contar con un HIPS.
- El producto debe ser capaz de bloquear aplicaciones por nombres del ejecutable, o por función hash (SHA-256)

6.2 GARANTIA COMERCIAL:

La garantía debe cubrir contra defectos de diseño y/o falla de funcionamiento de las licencias por el periodo de doce (12) meses, contabilizado a partir de la activación de las licencias. Dicha garantía cubre la atención de forma telefónica por las incidencias

de activación y/o funcionamiento de las licencias con un plazo máximo de respuesta de dos (02) horas, la misma que podrá ser brindada por el fabricante.

6.3 PRESTACIONES ACCESORIAS:

6.3.1. Mantenimiento preventivo: No aplica

6.3.2. Soporte Técnico:

- El postor ganador ofrecerá canales de comunicación (telefónicamente, portal de tickets de soporte y correo electrónico) para el reporte de incidencias.
- La entidad notificará incidencias del sistema según los canales de comunicación, teniendo el postor ganador 02 horas para la respuesta de atención de incidencias.
- Las incidencias deben solucionarse por el postor ganador en un plazo de 06 horas una vez recibido la respuesta de atención de incidencias. (Aquellos problemas que son generados por algún bug del producto están excluidos de este SLA).
- El postor ganador debe informar por correo electrónico y por cada incidencia reportada detallando:
  - Fecha y hora
  - Persona de contacto en la atención de la incidencia.
  - Descripción detallada del problema, su causa y solución encontrada.
  - Personal asignado para la resolución de este.
  - Problemas presentados durante resolución.
  - Documentación adjunta de los cambios hechos.
  - Recomendaciones
  - Fecha y hora de solución.
- El soporte estará cubierto por todo el tiempo de las licencias del antivirus, iniciaría al día siguiente de la firmado el acta de inicio de la implementación y activación.

6.3.3. Capacitación y/o entrenamiento:

- Se requiere curso con contenido oficial del fabricante, en la solución de antivirus adquirida.
- Los cursos deberán ser dictados por un especialista certificado en la herramienta ofertada y para un mínimo de cuatro (04) personas.
- La fecha de inicio de la capacitación será previamente coordinada y programada al día siguiente de firmado el acta de inicio de la implementación y activación dentro de los cinco (05) días, el tiempo de capacitación será de 08 horas como mínimo.
- Se emitirá un certificado por capacitación en la Administración del software.
- Se grabará el curso y será proveído al área de Sistemas.

7. REQUISITOS DEL PROVEEDOR:

7.1. Del Proveedor

- Persona natural con negocio o persona jurídica especializada en servicio y/o venta de software de protección y/o antivirus y/o malware y/o solución EDR.
- Contar con RNP vigente de corresponder
- RUC activo y habido (el proveedor deberá contar con actividad económica relacionada al objeto de la contratación)
- Contar con cuenta interbancaria CCI afiliado al RUC
- No contar con impedimento para contratar con el Estado, según el artículo 30 de la Ley General de Contrataciones Públicas

- **Experiencia:**

  Experiencia en la venta de bienes iguales o similares al objeto de la convocatoria, por un monto facturado acumulado no menor de S/ 50,000.00 (cincuenta mil y 00/100 soles), correspondiente a los últimos dos (2) años anteriores a la fecha de presentación de ofertas, computados desde la fecha de conformidad de la prestación o desde la emisión del respectivo comprobante de pago, según corresponda.

  Acreditación:
  La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

7.2. Del Personal

El postor deberá contar, como mínimo, con **un (01) profesional** que cumpla con el siguiente perfil:

- **Formación Académica:** Título profesional en Ingeniería de Sistemas y/o Ingeniería de Telecomunicaciones y/o Ingeniería Electrónica y/o carreras afines.

  Acreditación:
  Acreditar la formación académica con copia del grado académico u otro documento que demuestre fehacientemente lo solicitado.

- **Certificación:**
  Contar con certificación oficial vigente, nivel profesional o especialista, en la solución ofertada.
  La certificación deberá ser emitida directamente por el fabricante de la solución propuesta o por un Centro de Entrenamiento Autorizado debidamente acreditado por el mismo.

  Acreditación:
  Se acreditará con copia simple del certificado y/o constancia oficial emitida por el fabricante de la solución propuesta, o cualquier otro documento idóneo que permita verificar de manera fehaciente la certificación obtenida por el profesional.

8. LUGAR Y PLAZO DE ENTREGA:

8.1 Lugar:

La entrega de los bienes deberá efectuarse en el almacén de COFOPRI, ubicada en la Av. Paseo de la Republica N° 3135 - 3137, San Isidro, en horario de atención: de lunes a viernes de 08:30 a.m. a 1:00 p.m. y de 2:00 p.m. a 4:30 p.m o plena coordinación con la persona designada por la Oficina de Sistemas.

Asimismo, se menciona que la instalación debe ser realizada en las Sedes de La Molina y San Isidro, la instalación de la consola principal se realizara en la Sede de La Molina por la persona designada por la Oficina de Sistemas.

8.2 Plazo:

- **Plazo de entrega e Implementación:** La entrega del bien e implementación de la solución propuesta será hasta los quince (15) días útiles al día siguiente de notificado la orden de compra

- La solución ofertada, incluirá la configuración de la consola de administración.
- En lo posible la puesta en servicio de la solución ofertada se realizará sin afectar las labores normales de la institución y sin interrumpir la normal provisión de los servicios.
- Preparar la configuración de la consola o de paquetes de instalación para los equipos de sede remota.

➢ **Plazo de Ejecución:** El plazo de ejecución de la activación de la licencia de antivirus será de doce (12) meses, a partir del día siguiente de firmado el acta de la implementación y activación.

9. PRESENTACIÓN DE LOS ENTREGABLES

Entregable: El Contratista deberá presentar un Informe de la implementación y puesta en funcionamiento, donde se evidencie la activación de las licencias, las configuraciones realizadas y pruebas efectuadas en los servidores. Además de adjuntar el acta de la implementación y activación.

El plazo para la entrega del entregable es de cinco (5) días calendario, contados desde el día siguiente de haber terminado la implementación.

10. LUGAR DE PRESENTACION DE LOS ENTREGABLES:

Mesa de Partes Presencial del Organismo de Formalización de la Propiedad Informal (COFOPRI) ubicado en Av. Paseo de la República N° 3135 - 3137, distrito de San Isidro, provincia y departamento de Lima, o en Mesa de Partes Virtual en el siguiente link: http://mpv.cofopri.gob.pe/

Horario de atención, registro y trámite de la Mesa de Partes Virtual se encuentra habilitado durante las 24 horas del día; se consideran presentados en el día, aquellos documentos o solicitudes ingresados por la MPV entre las 00:00 horas hasta las 23:59 del día. De esta manera para el cómputo de los plazos inicia a partir del día hábil siguiente de la fecha en la cual presentó su documento o solicitud. El horario de atención de Mesa de partes presencial es de lunes a viernes de 8:30 a.m. a 4:30 p.m.

11. CONFORMIDAD DEL BIEN:

La conformidad de la adquisición será otorgada por el director de la Oficina de Sistemas y ésta será emitida en un plazo máximo de siete (07) días calendario después de terminada la implementación de la solución.

12. FORMA DE PAGO:

El Organismo de Formalización de la Propiedad Informal - COFOPRI, efectuará el pago de la contraprestación al contratista en un PAGO ÚNICO.

Para el trámite de pago el COFOPRI deberá contar con la siguiente documentación:

- Guía de Recepción firmada y sellada por el almacén de COFOPRI
- Comprobante de Pago, autorizado por la SUNAT.
- Carta de Garantía, de los bienes entregados.

El pago se realizará con abono en la cuenta “Código de Cuenta Interbancaria” (CCI) del contratista, El pago se realiza dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los bienes por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

13. PENALIDADES APLICABLES:

Penalidades por mora: Se aplicará a el/la proveedor/ a la penalidad establecida en el artículo 120° del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

Otras Penalidades:

N°	CONCEPTO DE PENALIDAD	PENALIDAD	PROCEDIMIENTO
1	Entrega del cumplimiento del informe de la implementación.	5% de la UIT vigente por cada día de retraso	Informe de conformidad de la Oficina de Sistemas

La suma de la aplicación de las penalidades por mora y de otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente

14. RESPONSABILIDAD POR VICIOS OCULTOS:

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

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

15. CLAUSULA DE CUMPLIMIENTO

15.1 **Conflicto de intereses (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.

15.2 **Declaración Jurada de Intereses**

Conforme al Artículo 2 de la Ley N° 31227 y su reglamento aprobado con Resolución de Contraloría Nº 158-2021-CG, constituye la presentación de la Declaración Jurada de Intereses, requisito indispensable para el ejercicio del cargo o función pública y demás situaciones que regula la presente ley, por lo que, su presentación debe realizar en los plazos establecidos, bajo sanción establecida en la Ley y su Reglamento.

En el marco de la Ley 31227, los sujetos considerados obligados, deberán presentar la declaración jurada de intereses a través del Sistema de Declaraciones Juradas para la Gestión de Conflictos de Intereses de la Contraloría General de la República, tanto al inicio como al cese de la contratación.

16. CLAUSULA ANTICORRUPCION Y ANTISOBORNO

El contratista declara conocer los compromisos antisoborno del COFOPRI, el cual se estable en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del COFOPRI:
https://cdn.www.gob.pe/uploads/document/file/2201691/RD%20N%C2%BA%20D000130-2021-DE.pdf.pdf

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 del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medias impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

17. MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCION EN LOS PROCESOS DE CONTRATACIÓN

En el COFOPRI promovemos la ética e integridad de la función pública, por lo que, si conoces de algún acto de corrupción ejercido por un/a servidor/a del COFOPRI, comunícanos tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/)

18. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, según el acuerdo de las partes; de conformidad con lo dispuesto en el artículo 81 de la Ley General de Contrataciones Públicas y del artículo 330 del Reglamento.
Cualquiera de las partes tiene derecho a iniciar la conciliación a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento.

19. RESOLUCION DE CONTRATO POR INCUMPLIMIENTO

El COFOPRI puede resolver el contrato, en los siguientes casos:

a) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
b) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
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 y antisoborno.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual y/o en la presentación de su cotización.
f) Cuando la suma de la aplicación de las penalidades por mora y de otras penalidades exceda el 10% del monto del contrato menor correspondiente.
g) Por agotamiento de la necesidad, previo sustento del área usuaria y/o área estratégica.

20. GESTION DE RIESGOS

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente requerimiento, 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.

COFOPRI
Firmado digitalmente por LEON INFANTES Leonardo Victor FAU 20306484479 soft
Motivo: Soy el autor del documento
Fecha: 11.03.2026 18:04:32 -05:00

FIRMA DEL RESPONSABLE DEL ÁREA USUARIA Y/O DEL ÁREA TÉCNICA ESTRATÉGICA