Requerimiento Especificaciones Técnicas

Órgano y/o Unidad Orgánica	Unidad de Tecnologías de la Información
Actividad del POI:	Ejecución de la Gestión de la Infraestructura Tecnológica y Comunicaciones.
Denominación de la contratación:	ADQUISICIÓN DE SOFTWARE MAS LICENCIAS DE ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO DEL PROGRAMA CONTIGO

I. FINALIDAD PÚBLICA

Contribuir en el cumplimiento de los objetivos y acciones estratégicas del Programa CONTIGO, optimizando los procesos y ejecución de la gestión pública para el desarrollo de las actividades administrativas que contribuya con una óptima operatividad de la Unidad de Tecnologías de la Información.

La presente adquisición busca adquirir una herramienta para la protección ante malware, virus y ataques informáticos en la Institución, el cual se ajuste y permita mantener y asegurar la información relevante del Programa CONTIGO.

II. OBJETIVO DE LA CONTRATACIÓN

La Unidad de Tecnologías de la Información requiere contar con una solución que permita garantizar la seguridad de los equipos de cómputo de los usuarios finales; de tal modo que pueda detectar, analizar y eliminar todo tipo de amenazas ya sea de virus, spyware, botnet, malware y variantes de estos.

III. CARACTERÍSTICAS Y CONDICIONES DE LOS BIENES A CONTRATAR

3.1 Descripción de los bienes a contratar

El Programa CONTIGO requiere el software más la suscripción por el periodo de 12 meses de un total de 202 licencias:

LICENCIAS	CANTIDAD
Servidores	20
Computadoras personales	182
TOTAL	**202**

La solución debe integrar únicamente productos de un solo fabricante. No se aceptarán propuestas que incluyan productos de fabricantes distintos.

El sistema de antivirus deberá detectar y eliminar en tiempo real, virus, gusanos, troyanos, macrovirus, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, ransomware y otros programas potencialmente peligrosos en todos los archivos residentes en memoria, comprimidos (cualquier formato de compresión, rar, zip, cab, arj, arz), ocultos y archivos de ejecución.

3.2 Características técnicas

3.2.1 Consola de Administración Centralizada.

3.2.1.1 Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes.

3.2.1.2 La consola de monitoreo y configuración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todos los componentes para el monitoreo y control de la protección de los dispositivos, así como la protección del correo electrónico y cifrado de discos.

3.2.1.3	El Fabricante de Seguridad debe ser líder en al menos los últimos 10 reportes de Gartner a nivel de Endpoint.
3.2.1.4	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.
3.2.1.5	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.
3.2.1.6	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
3.2.1.7	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
3.2.1.8	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.
3.2.1.9	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.
3.2.1.10	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.
3.2.1.11	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.
3.2.1.12	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.
3.2.1.13	Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
3.2.1.14	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
3.2.1.15	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
3.2.1.16	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
3.2.1.17	Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
3.2.1.18	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.
3.2.1.19	Capacidad de generación de informes, estadísticas o gráficos, tales como: Detalle de cuáles usuarios están activos, inactivos o desprotegidos, así como detalles de estos. Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
3.2.1.20	La solución deberá permitir la selección de la versión del software de preferencia, permitiendo así la prueba de la actualización sobre un grupo de PC's piloto antes de implementarlo para toda la red. También debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.
3.2.1.21	La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
3.2.1.22	Debe contar con el Idioma español en su interfaz Gráfica.
3.2.1.23	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.

3.2.1.24 Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.

3.2.1.25 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, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.

3.2.1.26 Una vez que se identifique un problema, debe permitir corregir los problemas de forma remota, con al menos las siguientes opciones:

- Proteger el dispositivo con la opción de inicio de una exploración.
- Forzar una actualización en ese momento.
- Ver los detalles de los eventos ocurridos.
- Ejecutar la comprobación completa del sistema.
- Forzar el cumplimiento de una nueva política de seguridad.
- Mover el equipo a otro grupo.
- Borrar el equipo de la lista.
- Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro manual o automáticamente.

3.2.1.27 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.

3.2.1.28 Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF.

3.2.1.29 Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints.

3.2.1.30 Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.

3.2.1.31 Consola/Servidor deberá provisionar doble factor de autenticación (2FA) para su interfaz web de administración; nativamente deberá ofertarse al menos en forma gratuita hasta cinco operadores y no deberá requerir de hardware/software que requiera pago o licenciamiento adicional.

3.2.1.32 No requerir licenciamientos adicionales de paga para su operación (excluyendo al sistema operativo), todo servicio y/o aplicación involucrada en el buen funcionamiento de consola web debe ser contemplado y no debe requerir licenciamiento adicional de paga al caso y/o bien licenciamiento “gratuito” no contemplado en el instalador inicial para implementación.

3.2.1.33 Debe proveer de tráfico seguro (HTTPS/SSL) para acceso a consola web.

3.2.1.34 Debe tener la capacidad de inspeccionar el tráfico seguro (HTTPS/SSL) para prevenir acceso a sitios maliciosos a través de conexiones cifradas.

3.2.1.35 La consola de administración web deberá tener la posibilidad de instalar un servidor local para reenvío de eventos (message relay) y cache en caso de que la maquina no pueda o no tenga permisos de navegación a internet que le impidan comunicarse con la consola en la nube.

3.2.2 Características Técnicas del Endpoint.

3.2.2.1 El endpoint antivirus deberá proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Sistema Operativo Windows, Linux y Mac el agente también deberá detectar PUA, adware y comportamiento sospechoso.

3.2.2.2 El endpoint antivirus deberá de contener protección integrada, es decir, en un solo agente tendrá como mínimo: control de amenazas, control de dispositivos, control de aplicaciones, control web, prevención de fuga

de información (DLP), gestión del firewall de Windows, protección contra virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).

3.2.2.3 Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.

3.2.2.4 Protección de malware fileless.

3.2.2.5 Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.

3.2.2.6 Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).

3.2.2.7 Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).

3.2.2.8 Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.

3.2.2.9 Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA).

3.2.2.10 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.

3.2.2.11 Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.

3.2.2.12 Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocidas.

3.2.2.13 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.

3.2.2.14 Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.

3.2.2.15 Protección de amenazas de día 0 a través de Inteligencia Artificial (Deep learning y signature les).

3.2.2.16 Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Inteligencia Artificial Deep Learning.

3.2.2.17 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.

3.2.2.18 Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.

3.2.2.19 Debe detectar el malware en un tiempo aproximado de no más de 20 milisegundos, debe indicarlo en la hoja de datos del producto.

3.2.2.20 Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.

3.2.2.21 La herramienta debe brindar la capacidad de realizar un 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.

3.2.3 Características de Protección Contra Ransomware.

3.2.3.1 Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas sino por algoritmos de Inteligencia Artificial.

3.2.3.2 Disponer de capacidad de remediación de la acción de cifrado malicioso de ransomware.

3.2.3.3 Debe poseer protección anti-ransomware para proteger archivos.

3.2.3.4 Debe poseer protección anti-ransomware para proteger el Master Boot Record.

3.2.3.5 Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware (rollback) sin requerir backup previo ni conexión permanente a internet o nube esta protección debe hacerse en el mismo agente de antivirus instalado en las maquinas.

3.2.4 Características de Protección Contra Vulnerabilidades y Técnicas de Explotación

3.2.4.1 Debe brindar detección y protección de al menos 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)
- EStack-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)

3.2.4.2 Mitigación de inyección de códigos en procesos.

3.2.4.3 Protección contra robo de credenciales.

3.2.4.4 Protección contra malware escondido en aplicaciones legitimas (code cave).

3.2.4.5 Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.

3.2.4.6 Evitar obtener escalada de privilegios y acceso elevado a recursos.

3.2.4.7 Modificación de las claves de registro para la ejecución de código arbitrario.

3.2.5 Funcionalidad de Control de Aplicaciones y Dispositivos

3.2.5.1 Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red.

3.2.5.2 Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.

3.2.5.3 Comprobar la identidad de una aplicación de manera genérica para detectar todas sus versiones. Permitir la solicitud de añadir nuevas aplicaciones en las listas de control de aplicaciones a través de interfaz web.

3.2.5.4 Prohibir a través de la política de inicialización de un proceso o aplicación basada en nombre y en el Hash del archivo.

3.2.5.5 Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.

3.2.5.6 Debe tener la opción de personalizar un mensaje que se mostrará al usuario en caso de bloqueo de ejecución de la aplicación.

3.2.5.7 Administrar el uso de dispositivos de almacenamiento USB (por ejemplo, unidades de disco duro y discos duros USB). Permitir, mediante reglas, el bloqueo o liberación de la lectura / escritura / ejecución del contenido de esos dispositivos.

3.2.5.8 Controlar el uso de otros dispositivos periféricos, como la comunicación infrarroja y el módem externo.

3.2.5.9 Las características del Control de Aplicaciones y Dispositivos deberán ser nativas del producto o incorporadas automáticamente por medio de plug-ins sin uso de agentes adicionales, siempre que sean desarrollados y distribuidos por el fabricante.

3.2.5.10 La gestión de estos dispositivos debe realizarse directamente la consola de administración con la posibilidad de definir políticas diferentes por grupos de endpoints.

3.2.5.11 Incorpore funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo con grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo.

3.2.5.12 Incorpore funciones avanzadas para el control de dispositivos mediante grupos de “dispositivos”, siendo posible asignarle reglas y/o directrices mediante grupos preestablecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo.

3.2.6 Funcionalidad de Protección y Prevención a la Pérdida de Datos (DLP)

3.2.6.1 Debe poseer protección de fugas o pérdida de datos sensibles, considerando su contenido o su tipo real, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.

3.2.6.2 Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y/o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido).

3.2.6.3 Posibilitar el bloqueo, sólo registrar el evento en la consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible.

3.2.6.4 Debe tener listas de CCL preconfiguradas con al menos los siguientes identificadores:

- Números de tarjetas de crédito.
- Números de cuentas bancarias.
- Números de pasaportes.
- Direcciones.
- Números de teléfono.
- Códigos postales definidos por países como: Francia, Inglaterra, Alemania, EE. UU, etc.
- Lista de correos electrónicos.

3.2.6.5 Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.

3.2.6.6 Permitir crear reglas de prevención de pérdida de datos por tipo de archivo verdadero.

3.2.6.7 Permitir el control de datos para al menos los siguientes medios:

- Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)
- Adjunto en el navegador (al menos IE, Firefox y Chrome).
- Adjunto en el cliente de mensajería instantánea (al menos Skype).

- Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD).

3.2.6.8 Posee la capacidad de autorizar, bloquear y confirmar el movimiento de datos sensibles y en todos los casos, grabar la operación realizada con las principales informaciones de la operación.

3.2.6.9 Capacidad de cobertura sobre todo tipo de datos y aplicación, no limitando ni restringiendo únicamente a un listado de compatibilidad otorgada por el fabricante.

3.2.6.10 Otorgue capacidad de protección extendida inclusive si el equipo se encuentra fuera de la red corporativa y no posee conexión a su respectiva consola de administración, garantizando en todo momento la no dependencia de la consola de administración para la protección funcional de todos los módulos incluidos a la solución DLP contratada.

3.2.7 Filtrado Web

3.2.7.1 La solución debe integrar la capacidad de Filtrado Web basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios.

3.2.7.2 La capacidad de Filtrado Web debe permitir y/o denegar el acceso URL estáticos mediante reglas configuradas.

3.2.7.3 La capacidad de Filtrado Web debe permitir el agrupamiento de las políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios.

3.2.7.4 La capacidad de Filtrado Web debe permitir la generación de logs y sincronización de estos a consola corporativa, de acuerdo con cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso. dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado, así como hora/fecha y descripción integra del evento.

3.2.7.5 Debe incluirse la capacidad de Filtrado Web sobre sitios URL que ocupen protocolo seguro (HTTPS).

3.2.7.6 Toda regla y/o política para el control URL, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en específico.

3.2.7.7 La herramienta deberá brindar el filtrado sin necesidad de instalación de agentes adicionales o complementos (Plug-In y/ Add-On) en los navegadores web.

3.2.7.8 Integre capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no debe requerir de instalación y/o módulo reflejado en componentes de programa en “Agregar quitar Programas -> Panel de Control”.

3.2.7.9 Incorpore capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación.

3.2.7.10 Faculte permitir y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering.

3.2.7.11 Provea posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios.

3.2.7.12 Integre capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no debe requerir de instalación y/o módulo reflejado en

componentes de programa en “Agregar quitar Programas -> Panel de Control”.

3.2.7.13 Integre capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no debe requerir de instalación y/o módulo reflejado en componentes de programa en “Agregar quitar Programas -> Panel de Control”.

3.2.8 La Herramienta debe tener Capacidades de XDR

3.2.8.1 El Analista debe poder identificar que atributos de código de un objeto son similares a archivos “known-good” y “known bad” con esto se puede determinar si se pueden permitir o bloquear.

3.2.8.2 Debe tener un sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints/servers con información detallada del malware y el origen de la infección (explorador de Windows, correo electrónico, navegador, etc.).

3.2.8.3 Debe permitir una investigación guiada entregando visibilidad de la dimensión del ataque cómo inicia, cómo impacta, cómo se responde.

3.2.8.4 Detectar ataques que pueden haber pasado desapercibidos.

3.2.8.5 Buscar de forma proactiva (Threat Hunting) indicadores de compromiso por nombre de archivo, SHA, direcciones IP.

3.2.8.6 Priorizar eventos para investigación.

3.2.8.7 Poder aislar una maquina comprometida de la red de forma automática mientras la investigación del incidente.

3.2.8.8 Poder generar un Snapshot forense durante una investigación de una amenaza.

3.2.8.9 Poder realizar búsquedas por “queries” de cualquier tipo de información.

3.2.8.10 Poder realizar queries de técnicas y tácticas de ataque mapeadas en MITRE ATT&CK.

3.2.8.11 Poder realizar queries de conexiones de Red y transferencias de archivos.

3.2.8.12 Poder realizar queries sobre información del SO, servicios, parches y más.

3.2.8.13 Poder realizar queries de actividad de usuario y autenticación.

3.2.8.14 Poder realizar queries de anomalías, actividad o conexiones de red inesperadas.

3.2.8.15 Poder realizar queries de eventos en los logs del sistema.

3.2.8.16 Poder realizar queries de actividad de procesos y reputación.

3.2.8.17 Poder realizar queries de detalles de archivos y acceso a archivos.

3.2.8.18 Poder realizar queries de accesos y cambios a llaves de registro.

3.2.8.19 Tener la capacidad de tomar control remoto de un equipo aislado utilizando una interfaz tipo CMD y de forma segura desde la misma consola de gestión para poder ejecutar comandos de sistema operativo y poder llevar a cabo el proceso de remediación.

3.2.8.20 La solución deberá ser capaz de realizar consultas basadas en lenguaje SQL para poder identificar comportamiento malicioso o hacer caza de amenazas (Threat hunting).

3.2.8.21 La solución debe poder almacenar los datos de los Indicadores de Compromiso detectados por la solución de EDR y XDR en la consola de gestión basada en nube en su data lake por un periodo de 30 días para poder llevar a cabo consultas de forma histórica y sin la necesidad que el equipo y/o servidor se encuentre en línea.

3.2.8.22 La solución debe contar con más de 200 consultas predefinidas para facilidad de la institución.

3.2.8.23 La solución debe poder personalizar o crear nuevas consultas para la personalización de esos indicadores de compromiso que le hagan sentido a la institución y poder detectar de forma temprana un posible evento de seguridad informático.

3.2.8.24 La solución debe poder calendarizar las consultas para que se puedan realizar en el horario que más le convenga a la institución y contar con los resultados de las consultas de forma periódica.

3.2.8.25 La solución debe poder incorporar capacidades avanzadas para mitigar riesgos extendidos que puedan ser identificados con facilidad mediante una solución específica del tipo Endpoint Detection and Response.

3.2.8.26 Deberá incorporar capacidades sofisticadas de detección y respuesta que permitan identificar comportamientos anómalos.

3.2.8.27 Funcionalmente deberá extender las capacidades de detección del endpoint local y al menos permitir detectar y/o responder ante:

- Detectar las amenazas persistentes avanzadas.
- Detener los ataques sin archivos (fileless).
- Bloquear las amenazas de 0-day.

3.2.8.28 Funcionalmente deberá ser capaz de indicar con precisión cualquier script ejecutado mediante powershell o CMD, dicha funcionalidad deberá proporcionar evidencia total de la línea de comandos ejecutada (strings del script y/o código fuente de este).

3.2.8.29 Deberá proporcionar una detección única basada en el comportamiento y en la reputación de archivos, dicha reputación de ficheros deberá estar al día y en constante evaluación mediante telemetría global, misma que deberá permitir en tiempo real evaluar la reputación del fichero, proceso o script analizado.

3.2.8.30 Deberá permitir configurar la sensibilidad de las reglas de detección para diferentes grupos de computadoras o usuarios, así como permitir eliminar fácilmente las falsas alarmas que pudiese causar alguna regla de detección manual incorporada por el equipo de seguridad de la información.

3.2.8.31 Deberá permitir combinar criterios como nombre de archivo, ruta, hash, paths, línea de comandos y firmante de aplicación con la finalidad de con precisión las condiciones de activación de las alertas.

3.2.8.32 Deberá permitir ubicar con facilidad cualquier comportamiento sospechoso inclusive para eventos pasados, mismo que deberá representarse por cualquier regla de detección nueva agregada.

3.2.8.33 Deberá permitir ubicar cualquier indicador de compromiso de forma tal que permita determinar si una amenaza ya existía antes de la emisión de alerta para alguna regla estática configurada.

3.2.8.34 Deberá incluir reglas de detección integradas, así como deberá permitir crear propias reglas para responder a los incidentes detectados.

3.2.8.35 Funcionalmente deberá permitir bloquear, detener o eliminar cualquier fichero o proceso mediante reglas de acción automatizadas o bien mediante intervención manual de algún operador de seguridad encargado internamente, dicha funcionalidad deberá ser extendida para ejecutar la misma acción sobre todos los computadores en forma simultánea.

3.2.8.36 Deberá permitir mayor visibilidad de lo ocurrido en cada computador respecto a ficheros, scripts y/o procesos en general.

3.2.8.37 Deberá proporcionar visibilidad total de lo ocurrido, siendo capaz de identificar el origen de una afección en particular, misma visibilidad deberá ser total y no solo representada en una imagen estática, posibilitando de dicha manera descubrir la naturaleza del origen y causa de afección.

3.2.8.38 Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).

3.2.8.39 Generación de excepciones ante falsos positivos.

3.2.8.40 Debe proteger el host incluso cuando este esté fuera de línea.

3.2.8.41 Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.

3.2.8.42 Disponer de capacidad de remediación de la acción de encriptación maliciosa de los ransomwares.
3.2.8.43 Debe poseer protección anti-ransomware para el sector de booteo.
3.2.8.44 Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
3.2.8.45 Debe informar a la consola todo el detalle del incidente para analizar la causa raíz de manera efectiva.
3.2.8.46 Protección contra vulnerabilidades y técnicas de explotación.
3.2.8.47 Detección y protección de técnicas de explotación de DLL Injection.
3.2.8.48 Mitigación de inyección de códigos en procesos.
3.2.8.49 Protección contra robo de credenciales.
3.2.8.50 Protección contra malware escondido en aplicaciones legitimas (code cave).
3.2.8.51 Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
3.2.8.52 Evitar obtener escalada de privilegios y acceso elevado a recursos.
3.2.8.53 Modificación de las claves de registro para la ejecución de código arbitrario.
3.2.8.54 La protección de la memoria y los módulos de control de la ejecución deben evitar las técnicas de ataque, pero sin limitarse a: Hijacking, File Injection, File Overflow, In-Memory execution, Explotación - Pivote de la pila, protección de la pila, código de la sobregrabación, raspadura de la RAM, payload malicioso, Inyección de Procesos - Asignación Remota de Memoria, Mapeo Remoto de Memoria, Escritura Remota a Memoria, Escritura Remota a Memoria EP, Código de Sobrescritura Remota, Unmap Remoto de Memoria, Creación de Hilo Remoto, APC Remoto, Escalamiento - LSASS Read y Zero Allocate.
3.2.8.55 El módulo de protección de memoria debe tener las siguientes acciones en caso de violación: ignorar, alertas, bloquear y terminar.
3.2.8.56 El módulo de scripting debería ser capaz de analizar al menos los siguientes lenguajes: PowerShell, Active Scripts, Jscript, WScript, CScript, Macros, VBA.
3.2.8.57 El módulo de control y análisis de secuencias de comandos debe tener las siguientes acciones en caso de violación: alertar y bloquear.
3.2.8.58 Si hay alguna identificación de código malicioso en los scripts, la herramienta debe actuar sobre el intérprete e impedir su ejecución inmediata.
3.2.8.59 De tener la capacidad para finalizar procesos y subprocesos en ejecución, si hay identificación de algún código malicioso ejecutándose en ellos.
3.2.8.60 Debe proporcionar funcionalidad de análisis de segundo plano para las amenazas de segundo plano, permitiendo escaneos periódicos de disco contra amenazas inactivas. Este análisis sólo se puede hacer cuando la estación / servidor está en modo inactivo, es decir, con los recursos disponibles para realizar esta acción.
3.2.8.61 Debe permitir exploración de amenazas sólo en los nuevos archivos.
3.2.8.62 Debe ser posible establecer el límite de tamaño para el análisis de archivos comprimidos.
3.2.8.63 Debe generar registro (log) de los eventos de detección de amenazas en ficheros locales, con opción de subir a la consola de gestión.
3.2.8.64 Debe generar notificaciones de eventos de amenaza a través de Syslog o alertas de correo electrónico.
3.2.8.65 Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc.
3.2.8.66 Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros.

3.2.8.67 Toda configuración a nivel de clientes deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.

3.2.8.68 Solución por contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO.

3.2.8.69 Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.

3.2.8.70 Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.

3.2.8.71 Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.

3.2.8.72 Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.

3.2.8.73 Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.

3.2.8.74 Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.

3.2.8.75 Comunicación entre clientes administrados (endpoints) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.

3.2.8.76 Solución por contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local.

- Incorpore tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.

3.2.8.77 Incorpore HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas, pero no limitadas requeridas:

- Bloquear archivos y/o aplicaciones para ejecución.
- Permitir ejecutar archivos y/o aplicaciones basadas en rutas de acceso y/o ficheros en particular.

- Bloquear archivos y/o carpetas contra escritura y/o acceso.
- Permitir escritura y/o acceso para archivos y/o carpetas.
- Bloquear escritura y/o modificación a llaves del registro de sistema.

3.2.8.78 Incorpore tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java.

3.2.8.79 Incorpore motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación.

3.2.8.80 Incorpore protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función deberá reflejarse en el componente HIPS cargado en el sistema.

3.2.8.81 Deberá incorporar protección especializada contra ataques del tipo ransomware, la misma deberá ser explícitamente visible dentro del apartado de configuración del producto final adquirido; específicamente el módulo especializado para la prevención del ransomware deberá detectar y bloquear procesos cuyo comportamiento encuadre con la conducta del ransomware en general.

3.2.9 Despliegue Agente

3.2.9.1 El cliente/agente para la instalación en estaciones de trabajo debe ser compatible con los sistemas operativos macOS 12, 13, 14 Intel-based Macs (64-bit) o superior, macOS 12, 13, 14 (Native) Apple Silicon M Series (ARM) o superior.

3.2.9.2 El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 10 (64-bit) y 11 (64-bit).

3.2.9.3 El cliente para instalación en servidores de Windows debe ser compatible con los sistemas operativos Windows Server 2016 en adelante.

3.2.9.4 Deberá ser compatible para su instalación en servidores con los sistemas operativos Linux siguientes:

- CentOS 7 (3.10.0-1062 or later)
- CentOS 8 Stream
- Ubuntu 18.04 (LTS) (4.15 or later)
- Ubuntu 20.04 (LTS)
- Ubuntu 22.04 (LTS)

3.3 Reglamentos técnicos o normas metrológicas y/o sanitarias

No aplica.

3.4 Acondicionamiento, montaje o instalación

Plan de Trabajo

El proveedor se reunirá con personal técnico de la Unidad de Tecnologías de la Información para realizar las coordinaciones relacionadas al objeto de la convocatoria, dicha reunión se realizará a partir del día siguiente hábil de la firma del contrato.

El proveedor entregará un plan de trabajo detallando las actividades a realizar, el diagrama topológico y/o configuración a implementar. La entrega de dicha documentación se realizará por Mesa de Partes de la entidad, sito en Av. Guillermo Prescott N° 490 – San Isidro – Lima - Lima en el horario establecido de las 8:30 am a 5:30 pm; o en su defecto, mediante la mesa de partes virtual https://sgd.contigo.gob.pe:8181/virtual/inicio.do, siendo el plazo tres (03) días calendario contabilizado desde el siguiente día hábil de firmado el contrato u emitido la Orden de Compra con el proveedor.

La Unidad de Tecnologías de la Información del Programa CONTIGO, dispondrá de dos (02) día adicional para aprobar dicho plan, la aprobación del plan trabajo podrá realizarse a través de correo electrónico dirigido al proveedor.

Acondicionamiento e Instalación
El proveedor deberá de realizar la instalación, configuración y puesta en funcionamiento de la solución ofertada.

Culminado el acondicionamiento y/o instalación y configuración **se deberá firmar un acta de implementación y operatividad de la solución**.

El plazo para el acondicionamiento y/o instalación y configuración de la solución será de diez (10) días calendario, contabilizados a partir del día siguiente de la entrega de las licencias de la solución ofertada en el almacén del Programa CONTIGO indicado en la orden de compra, sito en Av. Paseo de la Republica 3245 Edificio Senador – San Isidro – Lima.

3.5 Embalaje y rotulado:

3.5.1 Embalaje
No aplica.

3.5.2 Rotulado
No aplica.

3.6 Transporte
No aplica.

3.7 Garantía comercial
La solución ofertada tendrá una garantía y suscripción de licencia ofrecida por el fabricante por el periodo de doce (12) meses, contados desde el día siguiente de otorgado la conformidad de los bienes recibidos.

3.8 Muestras
No aplica.

3.9 Prestaciones accesorias a la prestación principal

3.9.1 Mantenimiento preventivo y/o correctivo
No aplica

3.9.2 Soporte técnico
El proveedor deberá disponer con una central de soporte técnico 24x7 durante el tiempo que dure la suscripción. El proveedor también brindará asistencia técnica fuera de este horario si el Programa CONTIGO tuviera alguna emergencia que guarde relación la solución adquirida.

El proveedor deberá atender cualquier incidencia o requerimiento de la Unidad de Tecnologías de la Información del Programa CONTIGO, que guarde relación la solución adquirida.

La atención para incidencias y/o requerimientos críticos deberán tener un tiempo de respuesta máximo de 30 minutos luego de reportado el inconveniente, el reporte se podrá realizar a través del teléfono, del correo electrónico o a través de la plataforma de mesa de ayuda del proveedor.

Las solicitudes de soporte técnico podrán ser atendidas de manera remota o presencial, según el personal técnico de la Unidad de Tecnologías de la Información lo determine.

3.9.3 Capacitación y/o entrenamiento

El proveedor deberá proporcionar un curso de mínimo 12 horas para tres (03) personas designadas por la Unidad de Tecnologías de la Información, la cual podrá realizarse en las instalaciones del Programa CONTIGO o de forma online mediante el uso de una plataforma virtual, el curso deberá ser el oficial de acuerdo al syllabus y/o guía del curso del fabricante, la asimismo al término de la capacitación, el proveedor entregará los certificados correspondientes a cada uno de los participantes, donde cada certificado deberá especificar como mínimo la el nombre completo del participante del curso y la cantidad de horas lectivas.

El instructor deberá ser un especialista que deberá contar con la certificación técnica oficial del fabricante de la marca de la solución ofertada, el cual será acreditada con el certificado respetivo y presentado en la etapa de suscripción del contrato.

3.9.4 Otras prestaciones accesorias

No aplica

3.10 Sistema de entrega

La entrega de los bienes será realizada en la sede central del Programa Nacional CONTIGO, Av. Guillermo Prescott N° 490 – San Isidro – Lima - Lima, de lunes a viernes, en el horario de 8.30 a 13:00 horas y de 14:00 a 17:30 horas.

3.11 Modalidad de pago

Suma Alzada

3.12 Seguros

No aplica

3.13 Disponibilidad de servicios y repuestos

No aplica

3.14 Lugar y plazo de ejecución de la prestación

3.14.1 Lugar

La entrega de los bienes se efectuará en el almacén del Programa CONTIGO, sito en Av. Guillermo Prescott N° 490 – San Isidro – Lima - Lima, en el horario laboral establecido de las 8:30 am a 5:30 pm.

3.14.2 Plazo

El plazo para la presentación del **Plan de Trabajo es de tres (03) días calendario** contabilizado desde el siguiente día hábil de firmado el contrato u emitido la Orden de Compra con el proveedor.

El plazo de la **entrega de las licencias será dentro de los diez (10) días calendario**, contabilizados a partir del día siguiente hábil de la notificación de la orden de compra.

El plazo para el **acondicionamiento y/o instalación y configuración de la solución será de hasta diez (10) días calendario**, contabilizados a partir del día siguiente de la entrega de las licencias de la solución ofertada en el almacén del Programa CONTIGO.

Los costos correspondientes al plazo de acondicionamiento, instalación y configuración de la solución corren por cuenta del contratista, sin que estos representen gasto alguno para la entidad.

IV. REQUISITOS DEL PROVEEDOR

El contratista deberá contar con los siguientes requisitos:

- Persona natural y/o jurídica.
- No tener impedimento para contratar con el estado, conforme al artículo 11° de la Ley de Contrataciones del Estado.
- Con RUC vigente ACTIVO y HABIDO.
- Registro Nacional de Proveedores (RNP) vigente.

PERSONAL CLAVE

1. **Jefe de Proyecto**

Perfil:

Un (01) jefe de Proyecto, debe de ser mínimo bachiller o Ingeniero Titulado de Sistemas y/o ingeniería de Telecomunicaciones y/o Ingeniería Electrónica y/o Ingeniería Informática y/o afines.

Acreditación:

La experiencia del personal clave se acreditará con copia del grado de bachiller o Título Profesional de Ingeniería.

Será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/.

Actividades:

Será encargado de la planificación, desarrollo y establecimiento de los tiempos durante la implementación de la solución ofertada.

Capacitación:

Deberá contar con certificación PMP y/o Certificación ITIL y/o Curso 27001.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) constancias o (ii) certificados o (iii) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

2. **Especialista en Implementación de Antivirus**

Perfil:

Un (01) Especialista en Implementación de Antivirus, debe de ser mínimo Profesional Técnico Titulado o Bachiller o Ingeniero Titulado en Ingeniería de Sistemas y/o Ingeniería de Telecomunicaciones y/o Ingeniería Electrónica y/o Ingeniería Informática y/o Computación e Informática y/o Redes y Seguridad y/o Informática y Sistemas y/o Redes y Comunicaciones de Datos y/o afines.

Acreditación: La experiencia del personal clave se acreditará con copia del grado de bachiller o Título Profesional de Ingeniería o Titulo Técnico.

Será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/ , según corresponda.

Actividades: A cargo de la Implementación de la solución y soporte durante la vigencia de la prestación.

Capacitación: El especialista en Implementación de Antivirus deberá contar con certificación del fabricante vigente y/o con certificación de entrenamiento de curso oficial de la solución ofertada.

Acreditación:
La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) constancias o (ii) certificados o (iii) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

El postor en su cotización debe acreditar un monto facturado acumulado equivalente a [DOS (2) VECES LA CUANTIA DE LA CONTRATACIÓN O DEL ÍTEM], por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia del [25% DE LA CUANTÍA], por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran bienes similares a los siguientes VENTA DE SOFTWARE ANTIVIRUS Y/O VENTA DE EQUIPOS Y PRODUCTOS DE SOFTWARE DE SEGURIDAD PERIMETRAL Y/O SOLUCIONES DE SEGURIDAD PERIMETRAL (FIREWALL DE RED) Y/O VENTAS DE PRODUCTOS DE SEGURIDAD NGFW Y/O ADQUISICIÓN DE STORAGE Y/O IMPLEMENTACIÓN DE EQUIPOS FIREWALL Y/O IMPLEMENTACIÓN DE EQUIPOS DE PROTECCIÓN PERIMETRAL Y/O VENTAS DE SOFTWARE.

V. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

5.1 Otras obligaciones

5.1.1 Otras obligaciones del contratista
No aplica

5.1.2 Otras obligaciones de la Entidad
No aplica

5.2 Adelantos
No aplica

5.3 Subcontratación
No aplica

5.4 Confidencialidad
No aplica

5.5 Medidas de control durante la ejecución contractual
No aplica

5.6 Conformidad

5.6.1 Área que recepcionará y brindará la conformidad
La recepción del bien estará a cargo de la Unidad de Tecnologías de la Información del Programa CONTIGO. La conformidad de la adquisición estará a

cargo de la Unidad de Tecnologías de la Información del Programa CONTIGO, para lo cual el proveedor deberá entregar los siguientes documentos:

- Plan de trabajo.
- Documentación que acredite las licencias solicitadas.
- Acta de acondicionamiento y/o instalación y configuración de la solución.
- Acta de capacitación.
- Informe detallado de la instalación y configuraciones realizadas.

La documentación debe ser remitida a la mesa de partes de la entidad, sito en Av. Guillermo Prescott N° 490 – San Isidro – Lima - Lima en el horario establecido de las 8:30 am a 5:30 pm, o en su defecto, mediante la mesa de partes virtual https://sgd.contigo.gob.pe:8181/virtual/inicio.do

5.6.2 Pruebas o ensayos para la conformidad de los bienes

No aplica

5.6.3 Pruebas de puesta en funcionamiento para la conformidad de los bienes

No aplica

5.7 Forma y condiciones de pago

Según lo señalado en el artículo 67 de la LGCP, precisa que el pago se realiza en un plazo máximo de diez días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

El Programa CONTIGO realiza el pago de la contraprestación pactada a favor del contratista en un único pago, previa conformidad del bien por parte de la Unidad de Tecnologías de la Información y a la entrega del comprobante de pago por parte del contratista, documentos consignados en el "*numeral 5.6, literal 5.6.1 Área que recepcionará y brindará la conformidad*".

El pago incluirá los impuestos de Ley y todo costo o retención que recaiga en el servicio, no debiendo proceder pagos a cuenta por servicios no efectuados, ni adelanto alguno.

La Entidad deberá pagar las contraprestaciones pactadas a favor del proveedor dentro de los diez (10) días calendario siguiente a la conformidad de la recepción del bien, siempre que se verifiquen las condiciones establecidas en la orden de compra o en el contrato.

5.8 Responsabilidad del proveedor

Señalado en el artículo 69 de la LGCP, en los contratos de bienes y servicios, el contratista es responsable por la calidad ofrecida y por los vicios ocultos por un plazo no menor de un año contado a partir de la conformidad otorgada por la entidad contratante.

5.9 Fórmula de reajuste

No aplica

5.10 Penalidades

Según el artículo 229.2 del RLGCP, la entidad contratante puede establecer penalidades en el contrato menor. La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

5.10.1 Penalidad por mora

Según el Art. 120 del RLGC, 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 consultorías de obras:
a) Para plazos menores o iguales a sesenta días: F=0.40
b) Para plazos mayores a sesenta días: F=0.25

5.10.2 Otras penalidades aplicables

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**

5.11 Garantías

Según el artículo 61 de la LGCP, el cumplimiento de las obligaciones de los contratistas debe ser garantizado a través de los mecanismos establecidos en la presente ley, a fin de cubrir el adelanto de pago, y el fiel cumplimiento del contrato, así como el fiel cumplimiento de las prestaciones accesorias.

5.12 Obligación 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 o personas vinculadas a las que se refiere la Ley General de Contrataciones de Públicas, 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, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a estas.

Además, el proveedor se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, el proveedor se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

5.13 Solución de controversias

Según el artículo 81.3 de la LGCP, en el caso de contratos menores, las partes pactan la conciliación como mecanismo de solución de las controversias.

5.14 Resolución de contrato por incumplimiento

Según lo señalado el artículo 68 de la LGCP, precisa que, cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

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.

5.15 Gestión de riesgos

Se deben identificar los riesgos que esta enfrenta en la contratación de bienes, dichas actividades y acciones se realizan sobre la base de la identificación, análisis, valoración, gestión, control y monitoreo de riesgos, que permiten tomar decisiones informadas y aprovechar las oportunidades potenciales derivadas de estos. Las entidades contratantes realizan la gestión de riesgos a fin de aumentar la probabilidad y el impacto de riesgos positivos y disminuir la probabilidad y el impacto de riesgos negativos, que puedan afectar el cumplimiento de la finalidad pública buscada. En todo momento, la gestión de riesgos debe considerar una mejora en la administración y en el uso de los recursos públicos.

5.16 Sanciones

El Tribunal de Contrataciones Públicas sanciona a los participantes, postores, proveedores, y subcontratistas, cuando incurran en las infracciones señaladas en el párrafo 87.1 del artículo 87 de la presente ley, sin perjuicio de las responsabilidades civiles o penales a que hubiera lugar.

Las sanciones por imponer pueden ser:
a) Multa.
b) Inhabilitación temporal.
c) Inhabilitación permanente.

La multa o inhabilitación que se impongan no eximen de la obligación de cumplir con los contratos ya perfeccionados a la fecha en que la sanción queda firme.

Asimismo, según el sub numeral 87.2 de la LGCP, para los contratos menores, solo son aplicables las infracciones previstas en los literales d), e), i), j), l) y m) del párrafo 87.1 del presente artículo.

Firma Digital
Programa CONTIGO

Firmado digitalmente por ALCALDE HUAMAN Hector FAU 20605733281 soft
Motivo: Soy el autor del documento
Fecha: 10.03.2026 11:17:15 -05:00

HECTOR ALCALDE HUAMAN
JEFE (e) DE UNIDAD
UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN