TERMINOS DE REFERENCIA PARA LA CONTRATACION DEL SERVICIO DE LICENCIA SOFTWARE ANTIVIRUS PARA LA MUNICIPALIDAD PROVINCIAL DEL CALLAO

I. DENOMINACION DE LA CONTRATACION

Servicio De Licencia Software Antivirus Para La Municipalidad Provincial Del Callao

II. AREA USUARIA

Oficina General de Tecnología de la Información y Telecomunicación

III. OBJETIVO

Contratar el servicio de antivirus corporativo para proteger los equipos y servidores institucionales frente a amenazas informáticas, garantizando la seguridad de la información y la continuidad operativa mediante una administración y actualización centralizada.

IV. FINALIDAD PUBLICA

Garantizar la seguridad de la información y la continuidad de los servicios tecnológicos de la Municipalidad Provincial del Callao, mediante la protección de los equipos y sistemas institucionales frente a amenazas informáticas, asegurando una adecuada atención a las áreas usuarias y a la ciudadanía.

V. ANTECEDENTE

La Municipalidad Provincial del Callao cuenta con infraestructura informática que soporta los sistemas institucionales, por lo que es necesario implementar medidas de seguridad ante amenazas como malware y accesos no autorizados. En ese sentido, se requiere la contratación del servicio de antivirus corporativo para proteger los equipos, servidores y garantizar la continuidad operativa y seguridad de la información institucional.

VI. DESCRIPCIÓN DE LAS ACTIVIDADES DEL SERVICIO

Servicio de 1000 Licencias de Software Antivirus, una Solución Unificada de Software Antivirus para Estaciones de Trabajo y Protección de Servidores que deberá constar de lo siguiente:

Nº Licencias	Características del Servicio
Servicio De 1000 Licencia Software Antivirus Para La Municipalidad Provincial Del Callao	**SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO.** • La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure). Ubuntu Desktop 20.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21,22 Apple macOS 13 y superior. • El producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo. • El producto ofertado debe contar con un sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado. • La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.

MUNICIPALIDAD PROVINCIAL DEL CALLAO O.G.TIT V°B°

	• La solución deberá contar con una funcionalidad antiransomware. • El producto ofertado debe contar con la funcionalidad de evitar que el malware dañe o deshabilite la protección antivirus, por lo que se puede estar seguro de que el sistema permanece protegido constantemente. • El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc. • Debe permitir elegir las unidades a escanear para los escaneos bajo demanda. • El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica. • El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. • El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia. • El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas. • El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario. • El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente. • La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS). • El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje. • El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes. • El producto ofertado debe tener la capacidad de tener un filtro web con un mínimo de 27 categorías entre las cuales se deba permitir o bloquear el acceso a las webs según el administrador lo disponga. • El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web. • El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo. • El producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario generar una lista de direcciones de correos permitidas o bloqueadas. • El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP. • La protección del correo electrónico en el cliente debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído. • El producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos cuando se trate de mensajes no deseados o detectados. • La solución deberá contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso total, evitando que los usuarios ingresen cualquier tipo de información. • El producto ofertado debe tener un módulo de protección para el acceso a la web para la detección y bloqueo de sitios web con contenido malicioso. • El producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.

MUNICIPALIDAD PROVINCIAL DEL CALLAO
OGTIT V° B°

	• El producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS. • El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems. • El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días). • El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo. • El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro • La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en aplicaciones como los navegadores web, lectores de PDF, clientes por correos electrónicos y Microsoft Office componentes. • La solución deberá contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa. • La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismos tradicionales. • La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada) • La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos de comando y control. • La solución deberá integrar un navegador seguro (Chrome), mostrando el logotipo de la solución presentada para asegurar que el módulo funcione correctamente, dando seguridad para proteger las transacciones bancarias, pagos en línea y sitios web. • La solución presentada incluirá una protección de la información ingresada con el teclado, contra registradores de pulsaciones al usar el navegador seguro. **SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES** Se debe considerar licencias de Antivirus, para todos los servidores, con las siguientes características: • La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 cuales deben tener compatibilidad con la firma de código de Azure. • El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 8 y 9; Ubuntu Server 22.04 y 24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15. • Compatible con versiones del kernel del sistema operativo Linux 4.14 y posteriores • El producto debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción realizada en el equipo (abrir, crear o ejecutar) • La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc • La solución deberá contar con una funcionalidad antiransomware.

MUNICIPALIDAD PROVINCIAL O.G. TIT V°B° CALLAO

	• El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. • El producto para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado. • El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica. • El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. • El producto debe contar con un agente que le permita ser administrado desde una consola centralizada. • El antivirus deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicaciones externas o de la consola de Administración. • La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo. • La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS). • El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje. • El producto debe permitir escanear archivos comprimidos. • Debe permitir elegir las unidades a escanear para los escaneos bajo demanda. • En sistemas operativos Windows, el antivirus deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA • La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, adicionalmente debe tener la capacidad de implementarse en forma On-premise. • La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en los puntos finales (Windows, Linux, Mac, Android). • Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración, de tal manera que se puedan agregar usuarios con diferentes niveles de acceso o permisos. • Por medidas de seguridad la consola de administración debe contar con un doble factor de autenticación para ingresar a la consola, que consiste en una contraseña permanente y una contraseña adicional o token de un solo uso. • La consola debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso luego de varios intentos fallidos de inicio de sesión. • La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari, Opera. • El servidor se deberá comunicar con los endpoints a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline. • El acceso a la consola a través del interfaz web se bloqueará de forma temporal (aproximadamente 10 minutos), luego de 10 intentos de inicio de sesión no satisfactorios, desde una misma dirección IP. • El producto debe ser capaz de mostrar los equipos detectados en la red.

MUNICIPALIDAD PROVINCIAL DEL CALLAO
OGTIT
V°B°

	• La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes. • El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas. • El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados /no actualizados y sistemas operativos administrados. • El producto debe permitir la instalación y desinstalación remota de la solución de seguridad con opción a desinstalar antivirus de terceros. • El producto debe permitir la generación de reportes gráficos y personalización de estos. • Los reportes deben ser fácilmente exportables en formatos CSV, PDF. • El producto debe contar con una herramienta capaz de escanear la red por Directorio Activo, Red IP o Dominios, o una tecnología propia de detección de equipos; en busca de nuevos equipos agregados a la red. • El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo. • Las actualizaciones deben ser descargadas directamente desde los servidores del fabricante y con la opción de usar repositorio instalado en un servidor compatible para que los clientes actualicen desde sus definiciones de virus, phishing, spam, bases de datos de URLs maliciosas, actualización de parches del producto entre otras. • Debe permitir gestionar licencias, ya sea como propietario de estas o como administrador de seguridad. Puede llevar un seguimiento de las licencias y los equipos activados con esta, además de observar sucesos relacionados con las licencias como son la caducidad, el uso y las autorizaciones. Esto sin necesidad de consultar la consola de administración. • La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o se cambie de equipo. • Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola. • Deberá permitir generar grupos de clientes dinámicos y grupos estáticos. OTROS: • El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región. • Que tenga oficinas de la marca en Latinoamérica y presencia local en el país. • El fabricante deberá haber ocupado una posición de Leader o Challenger en el Cuadrante Mágico de Gartner en el último año de publicación.

El proveedor deberá encargarse de la instalación de las 1000 licencias para la Renovación de antivirus de la Consola de Administración Centralizada de los Servidores de la Municipalidad Provincial del Callao en coordinación con la Oficina General de Tecnología de la Información y Telecomunicación como área usuaria.
Capacitación al personal técnico de la MPC durante 2 horas (10 personas) (Certificación y Capacitación por la casa matriz o distribuidor exclusivo)

El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región.
El fabricante deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación.

VII. REQUISITOS MINIMOS DEL PROVEEDOR

- No encontrarse inhabilitado para contratar con el Estado.
- Contar con RUC Activo y habido.
- Contar con RNP
- Persona Natural o Jurídica

VIII. PLAZO DE EJECUCION DEL SERVICIO

La instalación del servicio deberá ejecutarse en un plazo de hasta tres (03) días calendarios a partir del día siguiente de la notificación y o recepción de la orden de servicio, el plazo de la Licencia de antivirus será por 365 días. Contados a partir de la instalación del Servicio.

IX. CONFORMIDAD DE LA PRESTACION DEL SERVICIO

La conformidad de la prestación del servicio será brindada por la Oficina General de Tecnologia de la Información y Telecomunicación la cual se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

De existir observaciones, LA ENTIDAD debe comunicar las mismas a EL PROVEEDOR, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (02) ni mayor de ocho (08) días, dependiendo de la complejidad. Si pese al plazo otorgado, EL PROVEEDOR no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede resolver la ORDEN DE SERVICIO, sin perjuicio de aplicar las penalidades que correspondan, desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose las penalidades respectivas.

X. PENALIDADES

Si EL PROVEEDOR incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato. La Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{PENALIDAD DIARIA} = \frac{0.10 \times \text{Monto vigente}}{F \times \text{Plazo vigente en días}}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F 0.40.

b) Para plazos mayores a sesenta (60) días:

b.1) Para bienes, servicios en general y consultorías: F = 0.25

b.2) Para obras: F = 0.15

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

MUNICIPALIDAD PROVINCIAL DEL CALLAO O.G TIT V°B°

retraso. En el caso de sistemas de entrega de obra y consultoría de obra que contenga más de un componente el monto y plazo corresponde al componente que se ejecuta.

XI. RESPONSABILIDAD DEL PROVEEDOR:

EL PROVEEDOR es responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertados durante el tiempo que dure todo el plazo de ejecución del servicio.
La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

XII. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada.
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.

Nº	Descripción	% UIT
1	Demora a la solución de incidentes	2% de la UIT Cada Dia

XIII. CONTRAPRESTACION DEL SERVICIO Y/O FORMA DE PAGO

La forma de pago de proveedor prestador del servicio será en un pago único, el cual se realizará en moneda nacional, el mismo que incluirá todos los importes e impuestos de ley, y se efectuará después de ejecutada la respectiva prestación. Asimismo, para efectuar dicho pago, la entidad debe contar con la factura y conformidad correspondiente.

XIV. CONFIDENCIALIDAD

La confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros. El proveedor debe dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Esta obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido la prestación.

XV. DECLARACIÓN JURADA DEL PROVEEDOR

EL PROVEEDOR declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitada para contratar con el Estado en caso de incumplimiento.

XVI. RESOLUCIÓN DE LA ORDEN DE SERVICIO

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.
Cuando la resolución del contrato se produce por causa imputable a una de las partes, corresponde resarcir los daños y perjuicios acreditados.

En caso de corrupción de funcionarios o servidores no corresponde el pago de resarcimiento por daños y perjuicios al contratista, aun cuando este último no lo haya propiciado.
El reglamento establece las condiciones y procedimientos para resolver los contratos.

En el caso de los mecanismos diferenciados de adquisición para la contratación de tecnologías sanitarias para el diagnóstico y tratamiento de enfermedades raras y huérfanas, enfermedades oncológicas y de enfermedades de alto costo y en los contratos estandarizados de ingeniería y construcción de uso internacional, rige lo establecido en los respectivos contratos.

XVII. OBLIGACIÓN ANTICORRUPCIÓN Y ANTISOBORNO

La Entidad debe establecer las causales de solución de contrato, así como el procedimiento del mismo.
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.

MUNICIPALIDAD PROVINCIAL DEL CALLAO
OGTIT
V°B°

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, 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. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar

XVIII. GARANTÍAS.

EL CONTRATISTA entregará al perfeccionamiento del Contrato, la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD CONTRATANTE.

XIX. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes. Cualquiera de las partes tiene derecho a iniciar el arbitraje 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.

Facultativamente, Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas.

XX. GESTIÓN DE RIESGOS.

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

MUNICIPALIDAD PROVINCIAL DEL CALLAO
O.G. TIT
V°B°

XXI. LUGAR DE PRESTACIÓN DEL SERVICIO

El lugar de instalación del presente servicio será de acuerdo a las siguientes direcciones: Oficina de la Alta Gerencia de la Municipalidad Provincial del Callao sito en Av. Paz Soldán 252, Callao Horario de atención: lunes a viernes de 08:00 am a 1:00 pm – 2:00 pm a 4:30 pm.

XXII. MODALIDAD DE PAGO

A suma alzada