FORMATO Nº 01

TÉRMINOS DE REFERENCIA - SERVICIOS Y CONSULTORÍAS

Denominación de la Contratación:

CONTRATACIÓN DE LICENCIAS DE ANTIVIRUS PARA PC Y SERVIDORES

I. FINALIDAD PÚBLICA

Contar con una solución de seguridad de antivirus más contención que asegure la protección de los equipos de cómputo y servidores para que disminuya el riesgo de vulnerabilidades que pueda tener la infraestructura de la red causada por malware. De esta manera evitar que los servicios y funciones que se presta a todos los colaboradores de ENACO se vean afectados. Asimismo, la solución debe incluir herramientas de gestión de TI que permita tener el control de aplicaciones, control de dispositivos y realizar el mantenimiento de equipos y servidores de forma centralizada. La solución debe incluir un filtro Web que permita proteger a los usuarios de acceder a páginas con contenido malicioso.

II. ANTECEDENTES

El área de TIC contrató un software antivirus, el mismo que viene actualmente brindando la seguridad a todo el parque informático de ENACO, dicho producto ya cumplió su tiempo de licenciamiento. Motivo por el cual es necesario realizar una nueva contratación de un software antivirus más contención por un plazo de un año, que continúe brindando la seguridad necesaria y el correcto funcionamiento de los equipos de cómputo dentro de nuestra infraestructura tecnológica.

III. OBJETIVO DE LA CONTRATACIÓN

Contratar licencias de software antivirus más contención con la finalidad de mantener protegidos los equipos de cómputo de la entidad, ante posibles infecciones y/o vulnerabilidades producidas por los diferentes tipos de virus existentes en la red. Asimismo, prevenir la encriptación de la data causada por ransomware que viene afectando desde años anteriores y proteger a los usuarios de acceder a páginas con contenido malicioso.

.

IV. ALCANCES DEL SERVICIO

Para cumplir con el objetivo propuesto, se necesita contratar lo siguiente:

Software Antivirus Cantidad 160 Estaciones de Trabajo y 4 Servidores. TOTAL 164 licencias ANUALES.

Nuestras sedes están ubicadas en: Trujillo, Huancayo, Ayacucho, Lima, Cusco, Quillabamba y Juliaca.

Los equipos tienen instalados S.O Windows 7,8,10 o 11 de 32 y 64 bits

Los servidores tienen instalado S.O. Windows Server 2008 R2 o superior.

4.1. Herramientas de seguridad antimalware

La solución de seguridad deberá contar con herramientas antimalware que respalden exclusivamente al sistema de antivirus, estas herramientas deben incluir funciones específicas que garanticen la seguridad de la red corporativa.
La solución de seguridad de antivirus deberá integrar un motor de antivirus heurístico dedicado y basado en el comportamiento, un Firewall Cliente para el control del tráfico de RED LAN, un sistema de control que proteja a los procesos activos ante los ataques de bots y rootkits, un sistema de reconocimiento para prevenir la intrusión de hacking, hackers y spyware.
Asimismo, deberá incluir exclusivamente un sistema de contención del propio fabricante para evitar la propagación de nuevos malware desconocidos para el sistema de antivirus y su base de firma de virus.
El sistema de contención deberá ser una capa adicional de seguridad que respalde al sistema de antivirus cuando este no detecte ni elimine amenazas de malware del día cero.

4.2. Sistema de antivirus heurístico

El sistema de antivirus deberá instalarse o ser compatible en equipos con Windows XP/Vista/7/8, 8.1,10,11, Linux y Mac.

El sistema de antivirus deberá instalarse o ser compatible en servidores Windows Server 2003, 2008, 2012 y Linux y Mac.

La solución deberá soportar las versiones de 32 y 64 bits.

El sistema de antivirus deberá contar con una herramienta de detección que elimine los malware por comportamiento a través de su propia heurística y no basada en una lista de firmas de virus convencionales.

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) en no menos de 30 niveles, ocultos y archivos de ejecución.

El sistema de antivirus deberá contar con una tecnología Heurística propia avanzada que elimine al malware basado en su comportamiento malicioso en tres niveles (bajo, medio y alto) y no basándose en listas de vacunas de virus o en firmas de virus.

El sistema de antivirus deberá tener un módulo residente ejecutándose en la memoria del sistema (realtime) y un módulo de revisión de antivirus ejecutado en forma manual por demanda y por el usuario.

El sistema de antivirus deberá ser capaz de monitorear el comportamiento de Aplicaciones específicas para determinar el posible uso o intento de modificación de estas aplicaciones por agentes maliciosos y bloquear estas acciones mediante la contención y eliminarlo mediante el antivirus.

Las actualizaciones deberán realizarse de manera automática y/o manual desde la consola de administración y/o vía HTTP centralizada. Las estaciones de trabajo y servidores deberán actualizar exclusivamente de la consola de administración vía LAN y no actualizarse por ningún motivo a través del internet.

El sistema de antivirus deberá ser capaz de revisar llaves específicas del registro (regedit) del sistema operativo e impedir intentos de eliminación y modificación de escritura.

El sistema de antivirus deberá realizar escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas.

El sistema de antivirus deberá supervisar la actividad en tiempo real para controlar procesos avanzados.

El sistema de antivirus deberá ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o aplicación específica.

El sistema de antivirus deberá tener la capacidad de proteger al usuario de ataques de phishing, páginas webs con malware y páginas de estafa.

Los módulos para la detección de malware y phishing, deberán ser actualizables vía internet de manera programada o manual. De igual manera la propia aplicación deberá ser capaz de descargar parches críticos y aplicarlos automáticamente.

El sistema de antivirus deberá tener un módulo de protección en tiempo real para escanear la web y ser compatible con cualquier navegador.

El sistema de antivirus deberá detectar scripts maliciosos y bloquearlos.

El sistema de antivirus deberá ser capaz de revisar los macros de los documentos de office para de esta manera detectar actividad ilícita por parte de algún tipo de malware.

El sistema de antivirus deberá contar con una tecnología avanzada de desinfección, que le permita detectar y eliminar virus ya existente en la computadora.

El sistema de antivirus deberá contar con un módulo de cuarentena para restaurar archivos borrados por la heurística del antivirus. Esta función de restauración se debe realizar exclusivamente desde la consola de administración central y asimismo debe incluir esta función en el cliente final.

El sistema de antivirus deberá ser capaz de crear Discos o CDS de rescate, que permitan escanear particiones FAT Y NTFS.

El sistema de antivirus deberá contar con protección de la configuración que impida la modificación o desactivación por parte del usuario final. Esta protección deberá ser mediante contraseña.

El sistema de antivirus deberá contar con una herramienta que bloquee la manipulación de la configuración, la des habilitación de los módulos de seguridad y la desinstalación de la seguridad de antivirus.

El sistema de antivirus deberá tener las mismas funciones y características de escaneo que las estaciones de trabajo para los servidores, además debe proteger los servicios implementados en los mismos (Active Directory, Microsoft Exchange, Apache, Servidores ISA entre otros). Asimismo, debe proteger a los servidores Web, servidores de correos, servidores de dominios, servidores de base de datos, servidores de Backup entre otros.

El sistema de antivirus deberá contar con una herramienta de optimización de escaneo para los accesos a servidores (plataformas Linux y Windows), por lo que es necesario que los servidores en producción se encuentren totalmente protegidos y seguros.

El sistema de antivirus deberá ser capaz de monitorear el comportamiento de aplicaciones específicas, para determinar el posible uso o intento de modificación de estas aplicaciones por agentes maliciosos y bloquear estas acciones.

4.3. Firewall Cliente

El sistema de firewall cliente deberá ser del propio fabricante y que permita trabajar en distintos niveles de seguridad.

El sistema de firewall cliente deberá contar con reglas de aplicación en funciones de Denegar/permitir.

El sistema de firewall cliente deberá contar políticas que permitan un conjunto de reglas por puertos y protocolos.

El sistema de firewall cliente deberá contar con un filtro de sitios web.

La solución de firewall cliente deberá contar con un sistema que permita crear reglas seguras de aplicación.

El sistema de firewall cliente deberá contar con un filtro de tráfico de bucle, ARP e IP fragmentado.

El sistema de firewall cliente deberá contar con el soporte para protocolo IPv6.

El sistema de firewall cliente deberá controlar el tráfico de red LAN. Asimismo, debe tener la función de estabilizar y regular el tráfico de datos con el objetivo de evitar colapsos de red o desbordamiento de datos.

El sistema de firewall cliente deberá instalar un complemento en el driver de red en cada estación de trabajo para que de esta manera garantizar la seguridad contra ataques de hacking, spyware o bots.

4.4. Sistema de Contención

El sistema de contención deberá ser una herramienta que respalda al antivirus cuando este no detecta ni elimina nuevas amenazas de malware que son desconocidos o del día cero.

El sistema de contención deberá contar con un entorno especial donde las nuevas amenazas de malware que el antivirus no detecta y deja pasar las contiene y bloquea a nivel de red para impedir cualquier tipo de propagación e infección.

El sistema de contención deberá permitir dar privilegios al administrador de la red en decidir liberar o bloquear aplicativos que considere buenos o malos para su entorno de seguridad en la red.

El sistema de contención deberá ser administrado desde la consola de administración central.

El sistema de contención deberá contar con una función automática e inteligente para seleccionar archivos que irán a su entorno especial para ser analizados y excluidos de la red.

El sistema de contención deberá utilizar la virtualización de la CPU para no consumir recursos de hardware siempre que ésta disponga de core virtuales. De lo contrario, debe utilizar el aislamiento del proceso de espacio de usuario en tiempo de ejecución sin depender de la CPU.

El sistema de contención deberá contar con una interfaz que permite visualizar los procesos y archivos que se encuentras aislados en la contención.

El sistema de contención deberá permitir ingresar cualquier tipo de archivo ejecutable que contenga actividad maliciosa: ".exe, .dll, .sys, .cpl, .dll, .drv, .inf, .ocx, .pf, .scr".

4.5. Sistema de análisis dinámico del comportamiento de los procesos en ejecución

El sistema deberá tener la función de analizar y supervisar los procesos activos en tiempo real. Asimismo, debe tomar acción en eliminar o enviar a la contención.

El sistema de deberá liberar al proceso activo que se encuentra infectado por algún tipo de malware sin finalizarlo, sin eliminarlo o dañar el proceso mismo.

El sistema de deberá ser una capa adicional en la detección y eliminación de malware.

El sistema deberá generar alertas si se detecta actividad sospechosa.

El sistema deberá detectar malware del día cero mediante el análisis del comportamiento y las acciones de una aplicación. Si el comportamiento detectado corresponde a la de malware conocido, entonces el sistema debe generar una alerta que le permita poner en cuarentena la aplicación y deshacer los cambios que hizo.

4.6. Sistema de prevención contra intrusos

El sistema deberá prevenir los ataques de intrusión a red corporativa.

El sistema deberá tener la función de cerrar puertas traseras abiertas por malware de tipo bots, spyware, hacking y proxis anónimos.

El sistema deberá supervisar constantemente la actividad del sistema y sólo permitir a los ejecutables y procesos ejecutar si cumplen con las normas de seguridad vigentes que han sido forzadas por parte del administrador de red.

El sistema deberá proporcionar niveles extremadamente altos de protección sin la intervención del usuario.

El sistema deberá permitir a los administradores de red que buscan tener un control más firme en sus políticas de seguridad pueden crear rápidamente políticas personalizadas y conjuntos de reglas utilizando la interfaz de reglas.

El sistema deberá contar con la opción de monitoreo de actividades del sistema.

4.7. Sistema Verificación de archivos en la nube

La herramienta deberá contar con la función de análisis y verificación de archivos en línea analizando archivos desconocidos con un rango de verificaciones estáticas y de comportamiento para identificar aquellos que son maliciosos.

La herramienta deberá analizar todo el comportamiento en tiempo de ejecución de un archivo, para aumentar la efectividad de eliminar las amenazas del día cero que no detectaron los sistemas de detección basados en firmas de productos antivirus clásicos.

La herramienta deberá ser automática y dar una respuesta máxima ante el ataque de un nuevo malware desconocido a nivel mundial no mayor a un minuto.

La herramienta deberá contar con una consola propia que permita al administrador ver estadísticas reales de las nuevas amenazas detenidas y eliminadas por la solución.

La herramienta deberá permitir al administrador subir archivos para su análisis que se sospeche sea un malware dando una respuesta máxima de un minuto para su eliminación a nivel mundial.

4.8. Consola de administración centralizada

La consola de administración central deberá permitir la administración simultánea de equipos y servidores Windows, Linux y Mac.

La consola de administración central deberá ser en la nube. Esta consola deberá permitir administrar desde un solo punto administrar todas las oficinas y redes de la organización.

La consola de administración central deberá ser escalable, lo cual permitirá activar la administración de complejas redes, permitiendo la administración de más de 300 equipos desde un punto central.

La consola de administración central deberá sincronizarse con el

Directorio Activo para la instalación automática de la solución de seguridad en los equipos y servidores.

Asimismo, debe sincronizar con los grupos de trabajos de la red y permitir la instalación masiva en los clientes utilizando los rangos de IPs.

La consola de administración central deberá actualizar cada 15 minutos o menos y mantener al día todas las actualizaciones con los clientes.

La consola de administración central deberá permitir la administración basada en políticas y contener al menos políticas: Actualización, Opciones de Antivirus, opciones de contención, control de Aplicaciones y Firewall.

La consola de administración central deberá permitir crear políticas que se apliquen en las estaciones de trabajo, sobre el sistema operativo de maneja.

La consola de administración central deberá contar con filtros de control que permita detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad para garantizar la seguridad de la red.

La consola de administración central deberá permitir al administrador crear políticas desde la consola para evitar el uso de aplicaciones no deseadas, así como eliminar, autorizar y limpiar las mismas en los clientes.

La consola de administración central deberá contar con la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y Spyware.

La consola de administración central deberá permitir utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, grupo de trabajo, Active Directory y otros).

La consola de administración central deberá determinar los equipos que cumplan con las políticas centrales y/o que fueron modificadas localmente. Eventualmente puede "forzar" a los equipos a cumplir con las políticas centrales con tan solo un clic.

La consola de administración central deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico.

La consola de administración central deberá informar que tipo de malware fue detectado, en qué archivos, en qué computadores y que acción tomo al respecto.

La consola de administración central deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el Nombre del Equipo, Descripción, SO, Service Pack, IP, Grupo, Usuario que ha iniciado sesión, Última Actualización, Eventos de error, etc.

La consola de administración central deberá informar de los parches de actualización de Microsoft faltantes en el sistema operativo. Asimismo, debe permitir enviar la tarea de actualización de Windows update.

La consola de administración central deberá permitir crear grupos dentro de un grupo principal, con el fin de garantizar la administración ordenada.

La consola de administración central junto con la solución de seguridad para estaciones y servidores deberá ser de tipo Integrada; es decir incluir un único agente que brinde protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, detección Web de ataques de scripts maliciosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red. La consola de administración central deberá permitir la capacidad de múltiples políticas de configuración.

La consola de administración central deberá permitir la visibilidad global sobre todas las aplicaciones instaladas en todas las computadoras de la red con la capacidad de desinstalar de forma invisible los elementos no deseados.

La consola de administración central deberá permitir la visibilidad global de todos los servicios del cliente final con la capacidad de detenerlo, pausarlo e iniciarlo bajo demanda.

La consola de administración central deberá permitir la visibilidad global sobre todos los procesos que se ejecutan en todos los clientes finales con la capacidad de terminar procesos sospechosos o que consumen muchos recursos.

La consola de administración central deberá brindar la información sobre el cliente final: Usuario conectado y el tipo de sesión, todas las métricas de red, CPU / RAM / uso Swapfile, sistema operativo con Service Pack y la información de versión, las aplicaciones instaladas, procesos en ejecución.
La consola de administración central deberá Monitorear y alertar de un cliente final o servidor el exceso de uso de CPU, RAM, NIC, falta de espacio libre en el disco duro.

La consola de administración central deberá permitir la visibilidad de aplicación y el criterio de valoración del sistema de seguridad y registros de eventos con capacidad de exportación.

La consola de administración central deberá brindar el informe de estado del cliente final sobre las políticas de seguridad aplicadas.

La consola de administración central deberá brindar el informe de inventario de Hardware y Software instalados, detalladamente.

La consola de administración central deberá permitir el bloqueo de dispositivos de almacenamiento extraíble USB, óptico y floppy.

La consola de administración central deberá tener la opción para reiniciar, apagar y prender los equipos remotos.

4.9. Bloqueo de dispositivos

La solución de seguridad deberá contar con una herramienta que permita bloquear dispositivos ejemplos: Lector de CD y DVD, USB, bluetooth, card reader, lector de floppy, medios de almacenamiento por conexión USB por ejemplo: HDD externos, USB pendrive, almacenamiento de celulares Android, Iphone, Tablet, memorias SD entre otros esta política debe ser reflejada y administrada a través de la consola de administración centralizada.

4.10. Sistema de control de aplicaciones

La solución de seguridad de antivirus deberá contar con una herramienta que permita controlar aplicativos de las estaciones de trabajo y servidores, también debe generar políticas de bloqueo/permitir y eliminar utilizando exclusivamente el sistema de contención, esta función debe ser realizada únicamente desde la consola de administración centralizada.

4.11. Sistemas de alertas de hardware

La solución de seguridad de antivirus deberá contar con una herramienta que permita enviar alertas sobre el rendimiento de hardware de cada estación de trabajo y servidor, estas alertas deben informar sobre el uso excesivo de CPU, memoria RAM, tráfico de RED LAN y falta de espacio de HDD.

4.12. Sistema de administración y monitoreo remoto de equipos

La solución debe incluir software para solucionar y resolver problemas de forma

remota, permitiendo a los profesionales de TI acceder directamente a un sistema afectado, diagnosticar el problema y resolverlo sin necesidad de una presencia física.

4.13. Sistema de protección Web

La solución debe incluir software para controlar el tráfico web entrante y saliente , permitiendo o denegando el acceso a sitios web según listas y criterios como URL, palabras clave o calificación. La herramienta debe ser fácil de configurar y de bajo mantenimiento.

4.14. Consideraciones generales

Las licencias del software antivirus deberán ser identificados en todas sus características según las especificaciones técnicas y deberán estar a nombre de ENACO.
Las autorizaciones de uso serán entregadas como máximo a los cinco (5) días calendario contabilizados a partir del día siguiente de suscrito el contrato o recepción de la orden de compra.
La entrega de la licencia de software deberá incluir:
- Entrega virtual de las licencias y las credenciales de accesos a los correos asignados.
- Certificado de licenciamiento
- Manuales digitales en idioma original para la operación y administración.

De existir un problema con los medios de las licencias de software, se comunicará de inmediato al proveedor, el cual deberá brindar la atención y la solución al problema dentro de las veinticuatro (24) horas de recepcionada la notificación.
El postor debe contar con certificación de soporte del fabricante o ser representante del software antivirus
Garantía y soporte por todo el tiempo de licenciamiento de un (1) año
Soporte técnico in House y On Line.

4.15. Capacitaciones

Como parte de la solución presentada se requiere que el contratista imparta las siguientes capacitaciones:
Dos sesiones de dos (2) horas para el Administrador de la Consola, de forma virtual o videoconferencia.
Dos sesiones de dos (2) horas, para el personal de soporte TI ENACO, de forma virtual o videoconferencia.

V. MODALIDAD DE PAGO

La Modalidad de Pago aplicada será Suma Alzada.

VI. REQUISITOS DEL PROVEEDOR / PERFIL DEL CONSULTOR

- Persona Natural o Jurídica
- Que cuente con Registro Nacional de Proveedores- RNP.

- El postor debe acreditar un monto facturado acumulado equivalente a Diez mil Soles (S/ 10,000.00) por la venta de bienes iguales o similares al objeto de la convocatoria: Software Antivirus y/o herramientas de protección Web o de correo electrónico, durante los cinco (5) años anteriores a la fecha de la presentación de ofertas.

- Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compras, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher 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, correspondientes a un máximo de veinte (20) contrataciones.

VII. LUGAR Y PLAZO DE EJECUCIÓN

LUGAR: Calle Tenerías N° 103, Distrito de San Sebastián, Cusco.

PLAZO DE INSTALACION DEL SERVICIO: hasta 7 días calendario a partir del día siguiente de la notificación de la orden de servicio.

PLAZO DE EJECUCION DEL SERVICIO: 12 meses computados a partir del día siguiente de la instalación del servicio.

VIII. CONFORMIDAD

La conformidad será otorgada por Coordinador de TIC.

IX. FORMA Y CONDICIONES DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en Pago único
Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Documento del Coordinador TIC emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

X. CONFIDENCIALIDAD (De corresponder)

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 contratado, 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 el servicio. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos y demás datos compilados o recibidos por el proveedor.

XI. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de un (01) año), contado a partir de la conformidad otorgada por la Entidad.

XII. CONSIDERACIONES GENERALES A LOS PRODUCTOS (De corresponder)

Los derechos intelectuales de los productos y documentos elaborados por el proveedor que resulte seleccionado son propiedad de la Entidad, así como toda aquella información interna de la institución a la que tenga acceso para la ejecución del servicio.

XIII. PENALIDADES POR MORA

La penalidad por mora se aplicará conforme al Artículo 120° del Reglamento de la Ley General de Contrataciones Públicas – Ley 32069.

XIV. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

En caso de incumplimiento durante la ejecución contractual, la parte perjudicada podrá Resolver el Contrato conforme lo establecido en el literal b) del numeral 68.1 del Artículo 68° de la Ley General de Contrataciones Públicas – Ley 32069 y el numeral 122.1 del Artículo 122° de su Reglamento.

XV. SANCIONES

EL PROVEEDOR se compromete a cumplir las obligaciones derivadas del presente contrato, siendo aplicable lo previsto en el Artículo 87° de la Ley General de Contrataciones Públicas – Ley 32069.

XVI. CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO

EL PROVEEDOR sea persona natural, o en caso de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios o asesores, declara y garantiza no haber, directa o indirectamente, ofrecido, negociado o efectuado cualquier pago o, en general, entregado cualquier beneficio o incentivo ilegal en relación a la contratación.

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 y antisoborno (abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio), de manera directa o indirecta; a cualquier miembro del Directorio, funcionarios públicos, empleados de confianza, servidores públicos; así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor estimado, elaboración de documentos del procedimiento de selección, calificación y evaluación de oferta, y la conformidad de los contratos derivados de dicho procedimiento.

Además, EL PROVEEDOR debe comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

XVII. GESTIÓN DE RIESGOS

La entidad realiza la gestión de riesgos en todas las etapas de la contratación de acuerdo con toda la información obtenida, 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.

XVIII. SOLUCIÓN DE CONTROVERSIA

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación, son resueltos mediante conciliación.

XIX. APLICACIÓN SUPLETORIA

La Entidad aplica de manera supletoria el Código Civil, siempre que no se

contradiga con las disposiciones establecidas en los términos de referencia.

XX. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO (De corresponder)

En caso sea necesario que el proveedor realice alguna gestión en las oficinas de la Entidad, la Entidad debe indicar que protocolos sanitarios debe cumplir de acuerdo a la normatividad vigente y disposiciones particulares propias de la Entidad.

XXI. CUMPLIMIENTO DE LA LEY DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO, SU REGLAMENTO Y SUS MODIFICATORIAS

En mérito de los alcances de la Ley N° 27693, Ley que crea la Unidad de Inteligencia Financiera – Perú, y su Reglamento aprobado por Decreto Supremo N° 020-2017-JUS, así como la Ley N° 28306, Ley que modifica artículos de la Ley N° 27693, y demás normas modificatorias, en especial el numeral 7 del inciso 3.2 del artículo 3° del Decreto Legislativo N° 1249, LA ENTIDAD es considerada como sujeto obligado a reportar operaciones sospechosas y/o registrar operaciones de acuerdo al umbral que determine la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, e implementar un sistema acotado de prevención de lavado de activos y del financiamiento del terrorismo, toda vez que se trata de una empresa del Estado, que por la actividad que realiza no se encuentran dentro de los alcances del numeral 3.1 de la norma en cuestión.

En tal sentido, EL CONTRATISTA declara BAJO JURAMENTO, que se entiende prestado con la suscripción del presente contrato, que los recursos que componen su patrimonio no provienen de lavado de activos, financiamiento del terrorismo, narcotráfico, captación ilegal de dineros y en general de cualquier actividad ilícita.

EL CONTRATISTA manifiesta que los recursos recibidos en desarrollo de este contrato, no serán destinados a ninguna de las actividades antes descritas. Para estos efectos, EL CONTRATISTA autoriza expresamente a LA ENTIDAD para que, en caso detectara operaciones sospechosas la Unidad de Inteligencia Financiera – Perú (UIF-PERU), para que analice la información de operaciones sospechosas vinculadas a actividades de lavado de activos y/o de financiamiento del terrorismo para que proceda de acuerdo a ley y derive el reporte correspondiente a la Unidad de Inteligencia Financiera – Perú.

EL CONTRATISTA se obliga a realizar todas las actividades encaminadas a asegurar que todos sus socios, administradores, clientes, proveedores, empleados, etc., y los recursos de estos, no se encuentren relacionados o provengan, de actividades ilícitas, particularmente, de las anteriormente enunciadas.

XXII. AUDITORÍA

Siendo el objeto del contrato la prestación del servicio, ENACO S.A. queda facultada para auditar las actividades y controles asociados a la prestación del servicio contratado, considerándose que en este tipo de servicio requerido es de aplicación obligatoria lo establecido en la Ley Nº 29245 - Ley que regula los servicios de tercerización, cuyo objeto es regular los casos en que procede la tercerización, los requisitos, derechos y obligaciones, así como las sanciones aplicables a las empresa que desnaturalizan el uso de este método de vinculación empresarial.

XXIII. SUJECIÓN AL CÓDIGO DE ÉTICA DE ENACO S.A

La Empresa Nacional de la Coca Sociedad Anónima - ENACO S.A. declara que, como parte de sus actividades, cumple y hace cumplir las normas de su Código de Ética. De esta manera, pone en conocimiento su contenido en el link:

https://transparencia.enaco.com.pe/wp-content/uploads/2022/06/CODIGO-DE-ETICA-DE-ENACO.pdf

y exhorta que sus disposiciones se respeten -en todo tipo de contrataciones y en toda práctica comercial- entre todos los grupos de interés, en concordancia con el plan nacional de integridad pública y lucha contra la corrupción. Es pasible de denuncia todo acto contrario a la ética, despilfarro, fraude, abuso o acto corrupto, sin perjuicio de otras responsabilidades administrativas, civiles o penales, para lo cual puede hacer llegar su denuncia a www.enaco.com.pe.

AREA TECNICA ESTRATÉGICA / ÁREA USUARIA: INFORMATICA

FIRMA DIGITAL

Firmado digitalmente por: PAREDES GARCIA Humberto Leandro FAU 20114883230 hard
Motivo: Soy el autor del documento
Fecha: 22/09/2026 11:08:55-0500