TERMINO DE REFERENCIA Nº TDR-011176-2025-MIDAGRI-AGROMERCADO/OA-TI

1. ÁREA USUARIA

TECNOLOGIA DE LA INFORMACION

2. OBJETO DE LA CONTRATACIÓN

Contratación del servicio de licenciamiento de software antimalware y soporte técnico que permita la protección de la información almacenada en los equipos y sistemas informáticos de la entidad Agromercado

3. FINALIDAD DE LA CONTRATACIÓN

Mantener disponibles los sistemas de información, ante los diferentes tipos de ataques persistentes por malware, los cuales podrían dejar fuera de servicio los diferentes elementos de la infraestructura de TI que son consumidos por los usuarios internos y público en general.

4. ACTIVIDADES

El servicio incluye 300 licencias antimalware y soporte técnico por el periodo de un año. El producto ofertado debe ser bajo la modalidad llave en mano, debiendo realizar el proveedor como mínimo las siguientes actividades:

+ INSTALACIÓN
o Instalación y configuración On Premise de la Consola de Administración Centralizada y de las Aplicaciones de Seguridad correspondientes del producto ofertado
o La instalación y/o configuración del producto ofertado deberá realizarse en todos los equipos informáticos de la entidad, con sus respectivas licencias, tanto en la oficina central en Lima y sedes desconcentradas ubicadas en provincias
o Registro y despliegue de las actuales politicas y/o directivas de seguridad de la institución en los equipos informáticos
o Desinstalación del producto antimalware realizado por el contrato anterior
o Despliegue de las politicas, directivas de seguridad y/o tareas, a traves de la consola centralizada de admnistración de la solución ofertada.
o Deberá realizarse pruebas de funcionalidad entre la consola de administración y agentes antimalware

+ SOPORTE TÉCNICO
o El proveedor deberá contar con un medio para notificar las incidencias y/o requerimientos que se presenten que permita registrar mínimamente la siguiente información: fecha, hora, descripción del problema o requerimiento y contacto en la institución.
o El proveedor deberá generar un número de atención (ticket) en un máximo de 60 minutos, indicando la fecha y hora en que se recibió la llamada o se envió el correo, estos datos se tomarán para realizar el control de tiempos de respuesta
o El soporte técnico será solicitado por el especialista de la entidad en cualquier momento que se presente una incidencia de seguridad
o El soporte técnico será atendido de manera remota o presencial
o Se requiere 1 año de soporte para la consola de administración, 1 año de soporte en despliegue de agentes de red y antimalware, y 1 año de escalamiento de problema a fábrica del producto ofertado, siempre que sea necesario
o El soporte técnico deberá ser atendido de acuerdo a los siguientes tiempos: 2 horas de tiempo de respuesta y solución en atenciones vía telefónica, remota o por correo electrónico
o El soporte telefónico, apertura de ticket, incidentes graves, cambios de configuración y atenciones remotas deben ser 24×7
o El mantenimiento preventivo y correctivo debe ser 24×7

+ CARACTERÍSTICAS DEL SOFTWARE ANTIMALWARE
Protección de Estaciones de Trabajo:
1. La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft Windows: 8.1, 10 y 11; Ubuntu Desktop 22.04+; Apple macOS 13 y superior, y Android 11 o superior

2. Debe contar con un módulo de detección en tiempo real para proteger contra códigos maliciosos en cada ejecución, uso o creación de archivos
3. Debe contar con un sistema de detección de intrusos que analice el tráfico de red y bloquee el tráfico dañino
4. Debe permitir realizar un escaneo en modo seguro bajo línea de comando para la limpieza de virus
5. La solución debe ser capaz de detectar todo tipo de amenazas comunes, como virus, gusanos, troyanos, spyware, adware, rootkits, bots, y ransomware
6. Debe contar con una funcionalidad antiransomware
7. Debe evitar que el malware dañe o deshabilite la protección antivirus
8. El programa debe tener la opción de crear análisis bajo demanda que pueden ser programados para una fecha y hora futura o repetirse en intervalos
9. Debe permitir elegir las unidades a escanear para los escaneos bajo demanda
10. Debe ser capaz de crear exclusiones de escaneo por archivo, extensión o carpeta específica
11. Debe pedir una contraseña ante intentos de cambio indebidos en la configuración
12. El agente cliente debe poder ser administrado desde una consola centralizada y reportar el estado de todas las soluciones antivirus instaladas
13. Debe tener una funcionalidad que deshabilite las ventanas emergentes mientras la protección del sistema sigue ejecutándose en segundo plano
14. Debe poder catalogar procesos basados en la reputación en la nube, recopilando información anónima sobre amenazas detectadas
15. La solución debe tener un sistema de prevención de intrusiones basado en el host (HIPS)
16. Debe tener un filtro web con un mínimo de 20 categorías que permita bloquear o permitir el acceso a sitios web
17. Debe permitir crear grupos con múltiples URL para reglas de permiso y bloqueo
18. El bloqueo web debe poder asignarse por un rango de tiempo, por grupo y por equipo
19. Debe tener un filtro antispam que sea transparente con cualquier cliente de correo, como Microsoft Outlook y permita crear listas negras o blancas de correos
20. Debe analizar protocolos de e-mail POP3, IMAP, MAPI
21. La protección de correo electrónico debe permitir definir si se desea escanear solo el correo recibido, enviado o leído
22. Debe poder añadir una nota o etiqueta a los correos electrónicos recibidos o leídos cuando se detectan como no deseados o maliciosos
23. Debe contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso
24. Debe tener un módulo de protección en tiempo real para el acceso a la web
25. Debe ser capaz de escanear a través del protocolo SSL (HTTPS) para impedir la descarga de archivos infectados
26. Debe permitir realizar exclusiones de URL para que no sean analizadas por el antivirus en los protocolos HTTP y HTTPS
27. Debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos como USB.
28. Debe tener un módulo de control de dispositivos que permita crear varios grupos y aplicar reglas por un período de tiempo determinado
29. Debe contar con una primera exploración automática después de la instalación para asegurar que el equipo esté protegido desde el principio
30. Debe permitir exploraciones completas mientras el equipo no está en uso (bloqueado o suspendido.
31. Debe tener una herramienta para examinar el ordenador y determinar la causa de un comportamiento sospechoso, recopilando información detallada sobre los componentes del sistema
32. La solución debe poder realizar exploraciones en estado inactivo para brindar protección proactiva
33. Debe contar con la funcionalidad de bloqueo de exploits para evitar la explotación de vulnerabilidades en aplicaciones como navegadores web, lectores de PDF y Microsoft Office.
34. Debe tener un modo transparente que no muestre alertas cuando se está ejecutando una aplicación en pantalla completa.
35. Debe contar con un módulo de exploración avanzada de memoria para detectar amenazas sofisticadas.
36. El antivirus debe ejecutar un escaneo o exploración en cualquiera de los siguientes estados de la computadora: protector de pantalla activo, sesión de usuario bloqueada, o sesión de usuario finalizada
37. Debe contar con un módulo de protección contra Botnets para detectar conexiones con servidores malicioso
38. La solución debe incluir protección contra registradores de pulsaciones (keyloggers) en el teclado

Protección de Dispositivos Móviles

39. La solución deberá ser compatible con sistemas operativos Android 11 o superior.
40. Debe proteger en tiempo real contra malware, escaneando todos los archivos entrantes y salientes del equipo74.
41. Debe poder explorar durante la carga de batería y cuando la pantalla se encuentra bloqueada75.
42. Debe contar con una exploración bajo demanda para la desinfección de la memoria integrada y medios intercambiables.
43. Debe contar con protección contra la desinstalación con una contraseña de administrador.
44. La solución en función al cifrado de discos, deberá tener una configuración de seguridad para el dispositivo, incluyendo: establecer requisitos de complejidad de contraseñas, cantidad máxima de intentos de desbloqueo, vencimiento del código de bloqueo, temporizador de bloqueo, cifrado de contenido. En función de la protección para dispositivos móviles: bloqueo de cámara, notificaciones de GPS y detección frente a un dispositivo rooteado.
45. Debe permitir al administrador ejecutar comandos remotos desde la consola hacia los dispositivos moviles.
46. Respecto a los dispositivos móviles, debe bloquear remotamente dispositivos perdidos o robados.
47. Debe encontrar y rastrear remotamente el teléfono a través de coordenadas GPS.
48. Debe eliminar de forma segura contactos, mensajes y datos almacenados en la memoria interna y tarjetas SD.
49. Respecto a los dispositivos móviles, debe poder activar una alarma remota en el dispositivo, incluso si el volumen está en silencio.
50. Respecto a los dispositivos móviles, debe poder hacer un restablecimiento remoto de la configuración de fábrica.
51. Debe poder monitorear y bloquear el acceso a aplicaciones, e instar a los usuarios a desinstalarlas.
52. Debe poder bloquear páginas web mediante políticas de la consola administrativa.
53. Debe poder recibir un mensaje personalizado del administrador.
54. Debe bloquearse cuando se inserta una tarjeta SIM no autorizada.

Protección de Servidores de Red
Se deben considerar licencias de Antivirus para todos los servidores con las siguientes características:

55. La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012, 2012 R2, 2016, 2019, 2022.
56. Debe poder instalarse sobre plataformas x64 bits de Ubuntu Server 18.04, 20.04, 22.04 y 24.04 LTS
57. Debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción (abrir, crear o ejecutar)
58. La solución es capaz de detectar todo tipo de amenazas, como virus, gusanos, troyanos, spyware, adware, rootkits, bots y ransomwar
59. Debe contar con una funcionalidad antiransomware
60. Debe ser capaz de evitar que sus propios procesos, servicios y archivos sean detenidos, deshabilitados o modificados para garantizar su funcionamiento
61. En servidores Windows, se puede agregar exclusiones asociadas a aplicaciones y archivos críticos del servidor.
62. Debe ser capaz de crear exclusiones de escaneo por archivo, extensión o carpeta específica99.
63. Debe pedir una contraseña ante intentos de cambio de configuración indebidos
64. Debe contar con un agente que permita ser administrado desde una consola centralizada
65. La protección en tiempo real debe iniciarse con el sistema operativo y debe poder definirse qué tipos de medios serán analizados
66. El sistema HIPS debe tener los siguientes modos de configuración: automático e inteligente basado en políticas.
67. Debe permitir escanear archivos comprimidos
68. Debe permitir elegir las unidades a escanear para los escaneos bajo demanda
69. En sistemas operativos Windows, el antivirus debe contar con una herramienta integrada para inspeccionar componentes del sistema y determinar la causa de comportamientos sospechosos

SANDBOXING
70. Opcional. Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con SLA de 5 minutos hasta 1 hora de respuesta
71. Es posible crear una exclusión por ruta, detección y su hash (SHA-1)
72. Capacidad de sincronizar su licenciamiento con la nube y/o la consola de administración on-premise o en la nube
73. Cuando se detecta un archivo sospechoso ejecutado por primera vez, se debe mostrar una advertencia

74. Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fueron analizados
75. Debe tener protección proactiva, bloqueando el archivo/ejecutable hasta recibir el resultado del Sandbox en la nube.
76. Debe tener la capacidad de integrarse con la solución de antivirus o protección del punto final para mayores posibilidades de protección y aplicación de políticas.
77. Opcional. Enviar un archivo/ejecutable a través de una consola de administración del punto final.

Protección del Servidor de Correo Local
78. Debe poder soportar SO Microsoft Exchange Server y debe ser capaz de proteger hasta un total de 550 buzones. La solución antispam debe instalarse en un servidor distinto del servidor de correos.
79. Debe poder analizar los correos electrónicos para determinar si son legítimos o si poseen algún tipo de acción maliciosa
80. Debe poder ser AntiSpam
81. Debe poder ser Anti-Phishing
82. Debe poder permitir definir reglas de filtrado
83. Debe ser Antimalware y bloquear automáticamente archivos con detecciones maliciosas
84. Debe realizar cuarentena basada en la web.
85. La solución de seguridad debe explorar tanto el cuerpo como el asunto del correo electrónico para identificar vínculos maliciosos
86. Debe poder enviar mensajes a los usuarios afectados una vez que el correo electrónico se coloque en cuarentena
87. Opcional. Debe poder integrarse con sandboxing en la nube

Gestión de Parches y Vulnerabilidades
88. La solución deberá ser compatible con sistemas Windows 10 y 11
89. Debe rastrear activamente las vulnerabilidades de los sistemas operativos y aplicaciones comunes, e instalar automáticamente los parches en todos los endpoints
90. Debe poder configurar franjas horarias para la instalación automática de parches
91. Opcional. Debe detectar más de 30,000 vulnerabilidades y exposiciones comunes (CVE)
92. Debe poder explorar aplicaciones comunes como Adobe Acrobat, Mozilla Firefox y Zoom Client
93. Debe ser compatible con varias versiones de Windows
94. Debe priorizar y filtrar las vulnerabilidades según su puntaje de exposición y gravedad
95. Opcional. Debe admitir multi-inquilinos en entornos de red complejos
96. Debe permitir la visibilidad de vulnerabilidades en sectores específicos de la organización
97. Debe registrar y controlar las excepciones para los parches de aplicaciones seleccionadas
98. Debe proporcionar un inventario actualizado de parches con nombre del parche, nueva versión de la aplicación, CVE, gravedad/importancia y aplicaciones afectadas

Gestión de Consola Centralizada
99. La consola debe ser instalada en infraestructura On-premise
100. Debe permitir la configuración y administración remota de la solución antivirus instalada en los puntos finales (Windows, Linux, Mac, Android)
101. Debe permitir la delegación de tareas mediante la creación de usuarios con distintos perfiles y niveles de acceso
102. Por medidas de seguridad, la consola de administración debe contar con doble factor de autenticación
103. Opcional. Debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso después de varios intentos fallidos de inicio de sesión
104. La consola de acceso al servidor deberá ser 100% web y compatible con los navegadores: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari y Opera
105. 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
106. Opcional. El acceso a la consola a través de la interfaz web deberá bloquearse temporalmente después de varios intentos de inicio de sesión no satisfactorios desde una misma dirección IP
107. El producto debe ser capaz de mostrar los equipos detectados en la red
108. La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes
109. El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados sin

necesidad de consolas adicionales
110. El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red y mostrar reportes sobre: clientes con más amenazas, principales amenazas, clientes actualizados/no actualizados y sistemas operativos administrados
111. El producto debe permitir la instalación y desinstalación remota de la solución de seguridad, con opción a desinstalar antivirus de terceros
112. El producto debe permitir la generación de reportes gráficos y su personalización
113. Los reportes deben ser fácilmente exportables en formatos CSV y PDF
114. El producto debe contar con una herramienta capaz de escanear la red por Directorio Activo, Red IP o Dominios en busca de nuevos equipos agregados a la red
115. El producto debe ser capaz de generar alertas ante un evento específico mediante el envío de un correo
116. Las actualizaciones deben ser descargadas directamente de los servidores del fabricante, con la opción de usar un repositorio instalado en un servidor compatible
117. Debe permitir gestionar licencias, realizar un seguimiento de las mismas y de los equipos activados, y observar sucesos relacionados con las licencias
118. La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso de restauración del sistema o cambio de equipo
119. Deberá permitir la ejecución remota de scripts, archivos batch y paquetes personalizados de terceros a través de la consola
120. Deberá permitir mostrar el inventario de hardware de los equipos administrados
121. Deberá permitir visualizar los programas instalados en los equipos administrados y, si es posible, la desinstalación remota
122. Deberá permitir enviar notificaciones o mensajes unidireccionales a los equipos administrados
123. Deberá permitir crear y/o editar informes personalizados de los equipos administrados

5. ENTREGABLES

Nº	ENTREGABLE
1	- Informe técnico de la implementación con sus respectivas evidencias (capturas de pantalla) - Documento o certificado de la vigencia del producto ofertado. - Documento SLA y procedimientos de soporte técnico.

6. PLAZO DE EJECUCION

El proveedor contará con un plazo máximo de diez (10) días calendarios para ejecutar el servicio, contados a partir del día siguiente de notificada la Orden de Servicio. La vigencia del soporte técnico y licenciamiento del software antimalware será por 365 días calendarios contabilizados desde la activación de la licencia.

7. LUGAR DE LA PRESTACIÓN / EJECUCIÓN DEL SERVICIO

Av. General Trinidad Morán 955 Lince Lima 180

8. REQUÍSITOS DEL PROVEEDOR

- Deberá contar con el Registro Nacional de Proveedores del Estado vigente.
- Deberá acreditar experiencia mediante la presentación de facturas por un monto mínimo del doble del valor ofertado, relacionados con servicios objeto de la presente convocatoria.
- Deberá ser como mínimo partner plata o silver autorizado en el Perú del producto ofertado, acreditado mediante carta del fabricante y deberá aparecer en la página web del fabricante.
- El fabricante del producto ofertado deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica.

+ Personal clave:

- El responsable de la implementación deberá ser un profesional o especialista, con certificación técnica vigente emitida por el fabricante, con experiencia mínima de tres años en los últimos cinco años en instalación,

configuración y soporte del producto ofertado, acreditada mediante constancias de trabajo.
- La acreditación de la experiencia se computa con fecha de inicio y fecha fin o por el periodo de contrato que señala el documento.

Toda comunicación con la entidad es a través de la mesa de partes virtual con el CUT correspondiente de su notificación a la página https://sisged.agromercado.gob.pe/mpd

9. MATERIALES, EQUIPOS E INSTALACIONES REQUERIDOS PARA LA EJECUCION DEL SERVICIO

No aplica

10. RECURSOS Y FACILIDADES PROVISTAS POR LA ENTIDAD

La entidad brindará las facilidades para acceder a los servidores o equipos de cómputo donde se instalará la solución antimalware propuesto.

11. PRECIO / CONTRAPRESTACIÓN DEL SERVICIO

De acuerdo al mercado

12. MODALIDAD DE PAGO

El pago se realizará en una única armada, en moneda nacional, con depósito en cuenta interbancaria (CCI), previa presentación del informe de actividades y la conformidad correspondiente.

13. PENALIDADES

Penalidad por Mora: En ese caso incluye lo siguiente:

En caso de retraso injustificado en la ejecución de las prestaciones objeto de la Orden, se aplica automáticamente una penalidad por mora por cada día del retraso, calculado de acuerdo a la siguiente fórmula:
Penalidad Diaria = 0.10 x Monto

F x Plazo en Días

Donde F tendrá los siguientes valores:
- Para Bienes y Servicios, F = 0.40

Tanto el monto como el plazo, se refieren según corresponda, a la Orden, o en caso éste involucre obligaciones de ejecución periódica, a la prestación parcial que fuera materia del retraso.

14. OTRAS PENALIDADES

No aplica

15. RESPONSABLE DE DAR LA CONFORMIDAD

La conformidad estará a cargo del Encargado de las Funciones de Tecnología de la Información.

16. MODIFICACIÓN DE LA ORDEN DE SERVICIO

Cualquiera de las partes puede resolver, total o parcialmente el orden y/o contrato, de conformidad con el artículo 68 de la Ley N°32069, Ley General de Contrataciones Publicas, por caso fortuito o fuerza mayor que imposibilite de manera definitiva la continuación de la orden o por hecho sobreviniente al perfeccionamiento de la orden que no sea imputable a alguna de las partes o por mutuo acuerdo de las partes, siendo necesario para este último el visto bueno (V°B°) del área usuaria. Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de

prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

17. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Cualquiera de las partes puede resolver la orden por caso fortuito o fuerza mayor que imposibilite de manera definitiva la continuación de la orden o por hecho sobreviniente al perfeccionamiento de la orden que no sea imputable a alguna de las partes o por mutuo acuerdo de las partes, siendo necesario para este último el visto bueno (V°B°) del área usuaria. Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

18. DECLARACIÓN

Para efectos de la presente contratación, se deja en constancia de lo siguiente:
- Los servicios requeridos no pueden ser prestados por el personal de la entidad.
- Los servicios tienen carácter temporal o eventual (no permanente).

19. LEY DE SEGURIDAD Y SALUD EN EL TRABAJO

El proveedor del servicio debe cumplir con lo estipulado en la Ley N° 29783 y su Reglamento para la atención del presente requerimiento, de ser el caso.

20. PROTECCIÓN DE DATOS PERSONALES

El proveedor del servicio y la entidad declaran y reconocen que cualquier intercambio de datos personales que podrían contener datos sensibles que pueda producirse entre las partes, en el marco del cumplimiento de la prestación serán sometidas a los principios, medidas y disposiciones previstas en la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas.

En caso de que el proveedor del servicio transfiera a la entidad datos personales de sus colaboradores, clientes o de terceros en el marco de la ejecución de la prestación, el proveedor del servicio declara que para ello cuenta con el consentimiento libre, previo, voluntario, expreso, informado e inequívoco de cada uno de los titulares de los datos personales.

El proveedor del servicio, en el marco del cumplimiento de la prestación, podrá proporcionar a la entidad los datos personales de sus colaboradores, clientes o terceros para el tratamiento de los mismos, sin que ello implique la transferencia de los mencionados datos, asumiendo la entidad la condición de encargada del tratamiento de los datos personales proporcionados por el proveedor.

La entidad declara que los datos personales proporcionados al proveedor, así como aquellos generados o recopilados en el marco de la prestación serán tratados de forma confidencial y estarán sujetos a estrictas medidas de seguridad, conforme lo dispone la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas.

De la misma manera, en caso que la entidad proporcione datos personales o éstos deban ser recopilados o generados por el proveedor, en el marco del cumplimiento de la prestación, el proveedor del servicio declara conocer que asume la condición de encargado del tratamiento y, por tanto, se compromete a no utilizar o tratar los datos personales proporcionados, generados o recopilados con una finalidad distinta a aquella por la que le fueron entregados o por la que son generados o recopilados, así como a no transferirlos o divulgarlos a terceros, con excepción de entidades públicas que lo soliciten en el marco del cumplimiento de sus funciones debidamente sustentadas, o por el Poder Judicial cuando sea solicitado mediante orden judicial correspondiente, debiéndose notificar al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) dentro de las veinticuatro (24) horas de recibido el requerimiento. Asimismo, el proveedor de servicio

se compromete a que los datos personales proporcionados por la entidad serán tratados de forma confidencial y estarán sujetos a estrictas medidas de seguridad, en seguimiento de la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas.

En caso que la entidad y/o proveedor del servicio asuman la condición de encargados del tratamiento de datos personales que se pudieran proporcionar entre sí, se comprometen a conservarlos por el plazo de dos (2) años contados desde la culminación de la finalidad de la prestación, debiendo una vez vencido dicho plazo destruir los datos que se encuentren en su poder o en el de sus colaboradores o funcionarios, en un plazo no mayor a cinco (5) días hábiles.

La entidad y el proveedor del servicio declaran tener conocimiento y adherirse a las disposiciones previstas por la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas.

21. CLÁUSULA ANTICORRUPCIÓN Y ANTISOBORNO

EL PROVEDOR, 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 el artículo del Reglamento de la Ley General de Contrataciones Publicas, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

El/la proveedor/a acepta expresamente que él/ella, su(s) socio(s)a(s), o su(s) representantes(s) no llevará(n) a cabo acciones que están prohibidas por las leyes y otras normas de anticorrupción, así también se obliga(n) a no efectuar algún pago, ni ofrecer o transferir algún valor, o cualquier beneficio o incentivo, directa o indirectamente, a un funcionario(a) o empleado/a gubernamental o cualquier tercero/a relacionado/a con el servicio aquí establecido de manera que pudiese violar las leyes u otras normas anticorrupción, sin restricción alguna. Asimismo, el/la proveedor/a acepta conducirse, durante la ejecución de la prestación con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente, o a través de sus socios(as), accionistas, participantes, integrantes de los órganos de administración, apoderados/as, representantes legales, funcionarios(as), asesores/as y personas vinculadas, en concordancia a lo establecido en el artículo N°30 de la Ley N°32069 Ley General de Contrataciones Publicas. El/la proveedor/a, socios/as, o su(s) representante(s) se compromete(n) a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; además, de adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas. El incumplimiento de las mencionadas clausulas, durante la ejecución contractual, da derecho a que esta entidad resuelva automáticamente el contrato contenido en una orden de compra u orden de servicio y de pleno derecho, bastando la sola comunicación a el/la proveedor/a, o su(s) representante(s) informando el hecho y que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiere lugar.

22. DISPOSICIONES FINALES

En caso de presentarse aspectos no contemplados en los presentes términos de referencia, se aplicará de manera supletoria el Código Civil, así también como las normas y las leyes pertinentes que puedan ser aplicables.

23. RESPONSABILIDAD POR VICIOS OCULTOS

El plazo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de los servicios ofertados es de un (1) año contado a partir de la última conformidad otorgada.

24. TIPO DE INVITACIÓN

ABIERTA

25. JUSTIFICACIÓN DEL TIPO DE INVITACIÓN

26. CÓDIGO ÚNICO DE INVERSIÓN

27. DESCRIPCIÓN CÓDIGO ÚNICO DE INVERSIÓN
28. GARANTÍAS
No Aplica
29. 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 los artículos N°76 y N°77 de la Ley N°32069 Ley General de Contrataciones Publicas. El arbitraje será institucional y resuelto por Árbitro Único. LA ENTIDAD señala las instituciones arbitrales siguientes: 1.Centro de Arbitraje de la Cámara de Comercio de Lima. 2. Centro de Arbitraje y Resolución de Conflictos de la Pontifica Universidad Católica del Perú. 3. Cámara de Comercio Americana del Perú - AmCham Perú
30. GESTIÓN DE RIESGOS
Las partes realizan la gestión de riesgo de acuerdo con lo establecido en presente contrato, 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 de la contratación. Contratación de servicios: Al igual que en la compra de bienes, se podrían dar comportamientos irregulares como: (i) Favorecimiento indebido, (ii) Acceso a ventajas indebidas y (iii) Conflicto de intereses. (De corresponder el área usuaria, lo detallara en el numeral 4)
31. CLAÚSULA DE CUMPLIMIENTO
Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad

V°B°

AGROMERCADO

Firmado digitalmente por CORONADO CUMA Carlos Alberto FAU 20514859559 soft
Motivo: Doy V° B°
Fecha: 03.10.2025 11:19:34 -05:00