

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE DOS EQUIPOS APPLIANCE DE SEGURIDAD ANTISPAM PARA LA PROTECCIÓN DEL SERVICIO DE CORREO ELECTRÓNICO DEL MINISTERIO DE TRANSPORTES Y COMUNICACIONES

1 DESCRIPCIÓN DEL OBJETO

Adquisición de dos (02) equipos appliance de seguridad antispam que permitirán filtrar el contenido de los correos electrónicos de manera proactiva a fin de detectar elementos maliciosos que puedan afectar la disponibilidad del servicio de correo electrónico del MTC, ello en el marco de la inversión "Adquisición de equipos complementarios, servicios en la nube, software de respaldo de archivo y hardware en general; en la Oficina General de Tecnología de la Información en la localidad de Lima, distrito de Lima, provincia de Lima, departamento de Lima", con código N° 2577339.

2 OBJETIVO

Adquisición de dos (02) equipos appliance de seguridad antispam que permitirá la protección del servicio de correo electrónico del MTC, con la finalidad de contrarrestar las diferentes formas de amenazas que puedan afectar la disponibilidad del servicio tales como: suplantación de identidad (spoofing), correos no deseados (spam), phishing, virus, malware y otros que provengan de correos electrónicos maliciosos.

3 ANTECEDENTES

Los equipos de seguridad antispam del Centro de datos del Ministerio de Transportes y Comunicaciones tienen más de siete (07) años de antigüedad por lo que ya no cuentan con soporte técnico ni garantía del fabricante, y por lo tanto existe un alto riesgo de falla o avería del mismo causando la indisponibilidad del servicio de correo electrónico del ministerio, por lo que resulta necesario la adquisición de nuevo equipamiento por renovación tecnológica.

4 FINALIDAD PÚBLICA

Mantener los niveles de seguridad con la finalidad de proteger el servicio de correo electrónico del MTC, el cual es fundamental para todas las actividades relacionadas a la entidad.

5 ESPECIFICACIONES TÉCNICAS

Los equipos de seguridad antispam para la protección del servicio de correo electrónico del MTC, deberá regirse por lo indicado en las características y descripciones indicadas en el ítem 5.1.

ÍTEM	PRESTACIÓN	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
1	PRINCIPAL	EQUIPOS APPLIANCE DE SEGURIDAD ANTISPAM	2	Unidad
	ACCESORIA	Capacitación	1	Servicio
		Soporte Técnico	1	Servicio
		Mantenimiento preventivo	1	Servicio

Las especificaciones técnicas mínimas que debe cumplir son las siguientes:

5.1 CARACTERÍSTICAS DEL BIEN

5.1.1 PRESTACIÓN PRINCIPAL:

CARACTERÍSTICAS TÉCNICAS MÍNIMAS**1. Aspectos
Generales**

- a) Se deberá suministrar los dos (02) equipos appliance que proporcionarán el servicio de filtrado de correo y cifrado de mensajes de hasta 5800 casillas de correo electrónico con un licenciamiento de mil noventa y cinco (1095) días calendarios.
- b) Los equipos appliance antispam deberán poder configurarse para aceptar correo y reenviar el mismo a Office 365 u otros servicios similares de colaboración en nube mediante API o configuración nativa del fabricante.¹
- c) La solución de seguridad antispam debe basarse en "appliance" de propósito específico físico. No se tendrá en cuenta virtual appliances montados sobre un hipervisor o equipos de uso general (PCs o servidores) en la que se puede instalar y / o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux.
- d) Los dos (02) equipos appliance deberán operar en alta disponibilidad: activo-pasivo o activo-activo o balanceo de carga. Se deberá incluir el licenciamiento necesario para la alta disponibilidad.
- e) Los equipos appliance antispam deben soportar hasta 5,800 casillas tal y como se indica en el punto 5.1.1. literal a) de las especificaciones técnicas y que en caso el número de casillas aumente, se deberá considerar que los equipos deberán estar licenciados para soportar un crecimiento de hasta el 15%, equivalente a 870 casillas adicionales, durante la vigencia del contrato.²
- f) Los equipos appliance antispam deben soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema.
- g) Los equipos appliance antispam deben permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus y antispyware.
- h) Los equipos appliance antispam deben permitir retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
- i) Los equipos appliance antispam deben permitir definir el reenvío de correo (relay) a una IP específica con base a la IP origen del mensaje.
- j) Los equipos appliance antispam deben proporcionar soporte para múltiples dominios de correo electrónico.
- k) Los equipos appliance antispam deben permitir la implementación de políticas por destinatario, por dominio, por tipo de tráfico entrante o saliente.
- l) Los equipos appliance antispam deben ser capaces de entregar el correo en función de los usuarios existentes en una base de LDAP.
- m) Los equipos appliance antispam deben soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web o POP3.
- n) Los equipos appliance antispam deben ser capaces de programar el envío de informes de cuarentena.
- o) Los equipos appliance antispam deben ser capaces de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción, así como también en el título del mensaje o parte del contenido.³
- p) Los equipos appliance antispam deben ser capaces de mantener la cola de correo (queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega.
- q) Los equipos appliance antispam deben ser capaces de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP o que

¹ Consulta (44) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

² Consulta (45) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

³ Consulta (2) del pliego de consultas presentada por el participante SSG PERU S.A.C.

	<p>los equipos antispam puedan recopilar correos de servidores compatibles con POP3 e IMAP.</p> <p>r) Los equipos appliance antispam deben ser capaces de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados como no deseado, la cantidad de destinatarios con cuentas inexistentes o erradas.</p> <p>s) Los appliance antispam deben soportar al menos enrutamiento estático en IPv4 e IPv6, además de ser compatibles con el enrutamiento estático en IPv4 e IPv6⁴.</p> <p>t) Los equipos appliance antispam deben permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto.</p> <p>u) Los equipos appliance antispam deben tener características antispam, antivirus, antispyware y anti-phishing.</p> <p>v) Los equipos appliance antispam deben ser capaces de realizar la inspección del correo de Internet entrante y saliente.</p> <p>w) Los equipos appliance antispam deben contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger o la mejor opción que permita asegurar el despliegue de manera eficiente.</p> <p>x) Los equipos appliance antispam deben ser proporcionar protección contra ataques de denegación de servicio o que permita limitar la cantidad de sesiones por servidor o cliente SMTP y la cantidad de correos por sesión.</p> <p>y) Los equipos appliance antispam deben proporcionar un control DNS reverso para la protección contra los ataques spoofing.</p> <p>z) Los equipos appliance antispam deben ser capaces de permitir su configuración a través del acceso web (HTTP, HTTPS).</p> <p>aa) Los equipos appliance antispam deben ser capaces de permitir la creación de administradores únicos para la administración y configuración por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.</p> <p>bb) Los equipos appliance antispam deben ser capaces de proporcionar por lo menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)</p> <p>cc) Los equipos appliance antispam deben permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como antispam, antivirus, autenticación y entre otros de la solución ofertada.</p> <p>dd) Los equipos appliance antispam deben ser capaces de soportar doble factor de autenticación para el login de usuarios administradores, esta función debe estar disponible para al menos cinco (5) usuarios.⁵</p> <p>ee) Los equipos appliance antispam deben ser capaces de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).</p> <p>ff) Los equipos appliance antispam debe permitir generar informes de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.</p> <p>gg) Los equipos appliance antispam deben permitir generar informes por demanda o programados a intervalos de tiempo específicos</p> <p>hh) Los equipos appliance antispam deben permitir generar y enviar informes en formato PDF o HTML.</p> <p>ii) Los equipos appliance antispam deben soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II) o que los equipos antispam soporten el monitoreo por SNMP.</p> <p>jj) Los equipos appliance antispam deben permitir añadir un "descargo de responsabilidad" o disclaimer a los correos entrantes y salientes. El disclaimer podrá ser personalizado tanto en contenido, idioma y ubicación (al inicio del mensaje o al final del mensaje).</p> <p>kk) El disclaimer deberá poder ser aplicado por dominio.</p>
--	--

⁴ Consulta (46) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

⁵ Consulta (47) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

2. Capacidad	<ul style="list-style-type: none">a) Los equipos deben contar con al menos 4 interfaces GE RJ45. No se aceptarán transceivers RJ45 sobre puertos SFP o SFP+b) Cada equipo debe contar con un almacenamiento mínimo de 2TB. El almacenamiento debe estar conformado mínimo por dos (2) discos en RAID 1. La retención de logs será por lo menos trescientos sesenta y cinco (365) días.⁶c) Cada equipo debe tener una altura mínima de 1U y máxima de 3U.d) Cada equipo debe contar con doble fuente de poder de tipo Hot-Swap.e) Debe soportar manejar como mínimo 25 dominios o subdominios. Esta capacidad no debe estar limitada por licenciamiento.f) Debe permitir crear como mínimo 1000 reglas o políticas de correo entrante o saliente.g) Debe poder analizar/procesar como mínimo 400 mil mensajes por hora con las funcionalidades de antispam y antimalware activos.
3. Características de seguridad.	<ul style="list-style-type: none">a) Los equipos appliance antispam se deben conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.b) Los equipos appliance antispam deben poder detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.c) Los equipos appliance antispam deben estar en la capacidad de detectar si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante.d) La revisión de URLs debe permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante.e) Los equipos appliance antispam deben contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correos recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM.f) Los equipos appliance antispam deben ser capaces de realizar análisis Heurístico y definir umbrales máximos de acuerdo con el comportamiento del correo y así determinar si un correo es spam.g) Los equipos appliance antispam deben ser capaces de realizar análisis Bayesiano para determinar si un correo es spam.h) Los equipos appliance antispam deben ser capaces de detectar si el correo electrónico es un boletín de noticias (Newsletter).i) Los equipos appliance antispam deben contar con una técnica que detecten SPAM mediante el uso de Greylist o cualquier otra tecnología para la detección de spam en base al comportamiento de inicio de sesiones de correo.j) Los equipos appliance antispam deben ser capaces de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje.k) Los equipos appliance antispam deben ser capaces de realizar análisis sobre la base de palabras prohibidas (Banned Words).l) Los equipos appliance antispam deben contar con diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM.m) Los equipos appliance antispam deben permitir crear listas blancas o negras de palabras.n) Los equipos appliance antispam deben permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobrescribir el destinatario, archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado.

⁶ Consulta (32) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.
Consulta (48) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

	<ul style="list-style-type: none">o) Los equipos appliance antispam deben ser capaces de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM, esta característica deberá estar licenciada durante todo el periodo de garantía⁷.p) Los equipos appliance antispam deben ser capaces de soportar las listas negras de terceros tales como DNSBL, SURBL o similar.q) Los equipos appliance antispam deben ser compatibles con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6.r) Los equipos appliance antispam deben ser capaces de detectar las direcciones IP falsificadas (Forged IP).s) Los equipos appliance antispam deben permitir identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el análisis de las siguientes extensiones GIF, JPEG, PNG.t) Los equipos appliance antispam deben ser capaces de filtrar y analizar los archivos adjuntos y el contenido del e-mail.u) Los equipos appliance antispam deben ser capaces de ejecutar el análisis antivirus / antispymware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ, and RARv) Los equipos appliance antispam deben contar con una base de datos de malware suministrada por el fabricante y terceros aliados, la cual puede ser actualizada recurrentemente.w) Ante la detección de un malware, los equipos appliance antispam deben ser capaces de ejecutar las siguientes acciones: enviar un mensaje de notificación en lugar del correo, reenviar el correo y el malware a una cuenta definida, reescribir el destinatario.x) Los equipos appliance antispam deben contar con capacidades de evaluar, retener y/o bloquear correos que cuenten con amenazas avanzadas, Dia-Zero mediante el análisis de archivos con herramientas de Sandboxing.y) Debe permitir el análisis de sandboxing con soluciones on-premise o en la nube, sea del fabricante o de terceros.z) Deberá incluir el licenciamiento para enviar archivos adjuntos a la herramienta de Sandboxing.aa) El servicio de Sandboxing deberá poder analizar como mínimo archivos con las siguientes extensiones: docx, dotx, docm, dotm, MS Excel: xlsx, xlsxm, xltm, xlsb, xlam, pptx, ppsx, potx, sldx, pptm, ppsm, potm, ppam, sldm, JAR, PDF, .scr, .dll, .com, and .exe, .RAR y .ZIPbb) Los equipos appliance antispam deben ser capaces de reescanear los correos que son liberados de la cuarentena de SPAM por el usuario en busca de contenido malicioso.cc) Los equipos appliance antispam deben ser capaces de analizar el contenido y adjuntos de un mensaje en busca de palabras que indiquen que el correo deba ser puesto en cuarentena, Cifrado, Archivado, Bloqueado, Taggeado, sobrescrito o reenviado a otro host.dd) Los equipos ofrecidos deben incluir capacidades de DLP para evitar la fuga de información (Canadian SIN, US SSN, Credit card, ABA Routing, CUSIP, ISIN y diccionarios personalizados) y también evitar la fuga de archivos considerados confidenciales a través de correo.ee) Debe poder inspeccionar archivos protegidos por contraseña, mediante password predefinidos, una lista de contraseñas o buscar en el cuerpo la palabra password.ff) También debe contar con un componente de DLP para detectar la información sensible que puede estar llegando por e-mail. Se aceptará que esta función sea realizada en un equipo o solución aparte implementado de manera local.gg) La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares.hh) La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros.
--	---

⁷ Consulta (52) del pliego de consultas presentada por el participante SECURE TECHNOLOGIES S.A.C.

	<ul style="list-style-type: none">ii) La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.jj) La funcionalidad DLP para permitir la creación de filtros por tipos de archivos;kk) La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico.ll) La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado.
4. Reportes	<ul style="list-style-type: none">a) Deberá generar reportes bajo demanda o reporte calendarizados en intervalos específicos.b) Los reportes pueden ser generados y enviados como PDF o HTML.

El contratista deberá remitir al correo electrónico usrsegurinf@mtc.gob.pe el plan de trabajo que incluya el cronograma de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam. Dicho plan deberá ser remitido como máximo al 5to día contabilizado a partir del día siguiente de firmado el contrato, para su respectiva aprobación por parte de la Oficina de Infraestructura Tecnológica y Seguridad Informática.

5.2 REQUISITOS DE LA OFERTA

Las especificaciones técnicas de los dos (02) equipos appliance antispam relacionadas a: aspectos técnico, capacidad, características de seguridad y reportes, deberán ser sustentadas técnicamente con la siguiente documentación: folletos, y/o brochure, y/o hojas de datos, y/o manuales técnicos, y/o documentación técnica de acceso público (enlaces web). Para tal efecto deberá presentar los documentos en idioma español o en su defecto en idioma original con la respectiva traducción lo cual permita la validación del cumplimiento de cada especificación técnica de acuerdo a lo señalado en el ítem 5.1. Sólo se aceptará carta del fabricante para sustentar alguna característica técnica que no se encuentre en los documentos mencionados; dicha acreditación deberá ser emitida al postor y no a la entidad.⁸

5.3 PRESTACIONES ACCESORIAS

A) SOPORTE TÉCNICO

- El servicio de soporte técnico tendrá una vigencia de mil noventa y cinco (1095) días calendario, y se inicia a partir del día siguiente de la firma del acta de instalación y funcionamiento de los dos (02) equipos appliance antispam.
- Los dos (02) equipos appliance de seguridad antispam deberá contar con un periodo de licenciamiento de mil noventa y cinco (1095) días calendario, que comprende actualización de versiones, parches de seguridad, mantenimiento y soporte.
- El postor deberá contar con una mesa de ayuda para la prestación del servicio de soporte técnico, cuya modalidad a prestar es de 24x7 (24 horas del día, de lunes a domingo incluyendo feriados), con los recursos locales que el proveedor cuenta o con las acciones de escalamiento al fabricante, durante un periodo equivalentes a mil noventa y cinco (1095) días calendario.
- Ante cada reporte de anomalías, el proveedor deberá presentar al MTC un reporte por correo electrónico a la cuenta UsrSegurinf@mtc.gob.pe, que contendrá por lo menos la siguiente información:
 - Descripción detallada del problema, su causa y solución encontrada.
 - Problemas presentados durante resolución.
 - Documentación adjunta de los cambios hechos.
 - Recomendaciones
 - Fecha y hora de resolución.

⁸ Consulta (10) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.

Consulta (57) del pliego de consultas presentada por el participante SOFTSMART CORPORATION E.I.R.L

- Deberá tener un tiempo de respuesta y diagnóstico inicial de hasta cuatro (04) horas como máximo desde la comunicación por parte de la entidad mediante llamada telefónica y/o correo electrónico, es en este lapso de tiempo donde se registrará el ticket de atención de incidentes.
- Deberá tener un tiempo de solución de incidentes de hasta veinticuatro (24) horas como máximo el cual rige desde la comunicación por parte de la entidad mediante llamada telefónica y/o correo electrónico.⁹
- Se precisa que para incidentes que requieran escalamiento al fabricante, el plazo máximo de solución será de setenta y dos (72) horas.
- El soporte será On Site y On Line, en donde se atenderán incidentes relacionados a la plataforma implementada, asesoría, orientación técnica, auditoría y atención de requerimientos técnicos durante cualquier día de la semana, para ello la comunicación se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.
- Deberá brindar soporte técnico in situ a cargo de expertos profesionales en análisis de seguridad informática. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionadas de manera remota.
- El postor deberá garantizar que los equipos de seguridad antispam queden operativos y en óptimas condiciones luego de producida alguna falla.

B) **CAPACITACIÓN**

El proveedor deberá brindar un programa de capacitación con contenido oficial del fabricante del equipamiento ofertado, considerando lo siguiente:

- La capacitación deberá ser realizada por un especialista certificado en el equipamiento ofertado y para tres (03) colaboradores de la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.¹⁰

Perfil:

Formación académica:

- Mínimo Técnico Titulado en la carrera técnica de Electrónica y Telecomunicaciones, o Computación y Sistemas, o Computación e Informática de Sistemas, o Sistemas Empresariales, Informática y Sistemas, o Sistemas de Información, o Sistemas e Informática, Redes y Comunicaciones, o Sistemas, Cómputo y Telecomunicaciones, o Sistemas y Computación, o Electrónica, o Telecomunicaciones.¹¹
- Deberá contar con una certificación técnica emitida por el fabricante relacionado al producto ofertado.¹²

Acreditación:

- La formación académica se acreditará con la copia simple del grado o título requerido y la certificación, mediante copia simple del certificado respectivo.

La documentación para acreditar lo antes indicado deberá ser presentado para la firma del contrato.

- El proveedor deberá enviar vía correo electrónico como mínimo un (01) día antes de iniciar el curso, el plan de capacitación (syllabus) al correo electrónico UsrSegurinf@mtc.gob.pe para conocimiento de los participantes del programa.
- Deberá entregar el certificado de capacitación a cada uno de los asistentes.

⁹ Consulta (33) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.

¹⁰ Consulta (4) del pliego de consultas presentada por el participante SSG PERU S.A.C.

¹¹ Consulta (39) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.

¹² Consulta (59) del pliego de consultas presentada por el participante LOTENGO PERU S.A.C.

- La capacitación deberá tener un mínimo de 12 horas lectivas en modalidad presencial o virtual, las cuales serán desarrolladas en cinco (05) días calendario contabilizados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam.¹³
- El proveedor deberá brindar todo el material teórico sobre la capacitación en formato digital para cada asistente de la capacitación, Esta documentación deberá estar en español (como caso excepcional se aceptará en inglés aquella documentación técnica que no pueda ser traducida) y en formato HTML o PDF o WORD.

C) MANTENIMIENTO PREVENTIVO

- El contratista deberá realizar tres (03) mantenimientos preventivos, los cuales deberán realizarse cada trescientos sesenta y cinco (365) días calendario, dentro de los mil noventa y cinco (1095) días calendario contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam. El mantenimiento se podrá realizar en modalidad presencial o remota.
- El mantenimiento consta de actualizaciones de versiones del software, revisión de reglas de seguridad, revisión de eventos y/o incidentes de seguridad y todas aquellas recomendaciones que permitan optimizar el uso de los equipos de seguridad antispam.
- Al finalizar de cada mantenimiento preventivo, el CONTRATISTA deberá entregar un informe dirigido a la Oficina General de Tecnología de la Información, en el cual indique las acciones realizadas durante el mantenimiento y los tiempos llevados a cabo por cada actividad. También deberá adjuntar reportes con el siguiente contenido: Eventos, alertas y estado de salud del hardware.

5.4 GARANTÍA COMERCIAL

El contratista proporcionará un periodo de garantía de mil noventa y cinco (1095) días calendario por cada uno de los bienes adquiridos que componen los equipos appliance antispam, dicha garantía iniciará al día siguiente de emitida la conformidad de la entrega de los equipos.

La garantía debe cubrir el reemplazo de los equipos o partes por repuestos originales en caso de fallo y se deberá colocar un equipo de características similares o superiores hasta que se efectúe la revisión correspondiente; esto se deberá efectuar en un periodo no mayor a 24 horas a partir de la notificación de avería.

En caso de ser necesario y de aplicar el reemplazo del equipo por avería, el proveedor tendrá un plazo de hasta treinta (30) días calendario para realizar el cambio, el cual deberá ser de las mismas características o superiores.

5.5 MODALIDAD DE CONTRATACIÓN

Llave en mano-

6 LUGAR DE ENTREGA E INSTALACIÓN

6.1 LUGAR DE ENTREGA:

Almacén Central del MTC (Jr. Zorritos N°1203, Cercado de Lima).

El horario de atención del Almacén es:

HORARIO	MAÑANA	TARDE
	9:00AM – 12:00 HORAS	13:30 –16:30 HORAS

6.2 LUGAR DE INSTALACION:

Sede Central del MTC (Jr. Zorritos N°1203, Cercado de Lima).

¹³ Consulta (30) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.

7 **PLAZO DE EJECUCIÓN**

7.1 **PRESTACIÓN PRINCIPAL**

El plazo total de la prestación principal es de setenta y cinco (75) días calendario, contados a partir del día siguiente de la firma del contrato, divididos de la siguiente manera:

✓ **Plazo de entrega de los equipos**

El plazo máximo de entrega de los dos (02) equipos appliance de seguridad antispam deberá ser hasta sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato.

✓ **Plazo de instalación y puesta en funcionamiento de los equipos**

El plazo máximo de instalación y puesta en funcionamiento de los equipos appliance antispam será de hasta quince (15) días calendario, contados a partir del día siguiente de la entrega de los equipos.

Como máximo al día siguiente de concluida la etapa de instalación y puesta en funcionamiento de los equipos appliance antispam, se formalizará mediante la respectiva acta de instalación y puesta en funcionamiento de los equipos appliance antispam, suscrita de modo conjunto por el representante del contratista y el especialista designado por la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.

7.2 **PRESTACIÓN ACCESORIA**

Plazo de ejecución de la prestación accesoria:

Capacitación:

La capacitación se realizará en cinco (05) días calendario contabilizados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam por un total mínimo de 12 horas lectivas.

Soporte técnico

El soporte técnico es 24x7 durante los mil noventa y cinco (1095) días calendario, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam.

Mantenimiento preventivo

El mantenimiento preventivo deberá ser realizado cada trescientos sesenta y cinco (365) días calendario durante los mil noventa y cinco (1095) días calendario, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam.

8 **ENTREGABLES**

El contratista deberá remitir a la entidad los siguientes entregables como parte de la prestación principal y accesoria.

8.1. **PRESTACIÓN PRINCIPAL**

✓ **Entregable Único**

Será presentado hasta los siete (07) días calendario contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los dos (02) equipos appliance antispam, el cual consta de lo siguiente:

- Acta de entrega de los equipos appliance antispam conforme al plazo indicado en el numeral 7.1 junto con la guía de remisión de los equipos en donde se precise los datos y número de serie de los mismos.
- Documento que indique la matriz de escalamiento para reportar incidentes: Nombre del contacto técnico, correo electrónico, número de teléfono.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Secretaría General

Oficina General de
Tecnología de la
Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

- c. Documento en el cual se muestre la vigencia de la garantía de los equipos appliance antispam.
- d. Informe técnico final de la instalación y puesta en funcionamiento de los equipos appliance antispam.



8.2. **PRESTACIÓN ACCESORIA**

8.2.1. **Capacitación**

El proveedor deberá brindar el certificado de capacitación a cada uno de los participantes.

El plazo para la entrega de dicha documentación será de diez (10) días calendario, contabilizados a partir del día siguiente de haber concluido la capacitación.

8.2.2. **Soporte Técnico**

La presentación del entregable se efectuará cada trescientos sesenta y cinco (365) días calendario, contabilizados contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam. El CONTRATISTA deberá entregar los siguientes informes dirigidos a la Oficina General de Tecnología de la Información, los cuales constan de lo siguiente:

Entregable N° 01: Informe que indique las incidencias del soporte técnico dentro del primer año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam.

Entregable N° 02: Informe que indique las incidencias del soporte técnico dentro del segundo año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam.

Entregable N° 03: Informe que indique las incidencias del soporte técnico dentro del tercer año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam.

8.2.3. **Mantenimientos preventivos**

La presentación del entregable se efectuará cada trescientos sesenta y cinco (365) días calendario, contabilizados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam. El CONTRATISTA deberá entregar los siguientes informes dirigidos a la Oficina General de Tecnología de la Información, los cuales constan de lo siguiente:

Entregable N° 01: Informe que indique las acciones realizadas durante el mantenimiento preventivo y los tiempos llevados a cabo por cada actividad dentro del primer año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam. También deberá adjuntar reportes con el siguiente contenido: Eventos, alertas, estado de salud del hardware.

Entregable N° 02: Informe que indique las acciones realizadas durante el mantenimiento preventivo y los tiempos llevados a cabo por cada actividad dentro del segundo año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam. También deberá adjuntar reportes con el siguiente contenido: Eventos, alertas, estado de salud del hardware.

Entregable N° 03: Informe que indique las acciones realizadas durante el mantenimiento preventivo y los tiempos llevados a cabo por cada actividad dentro del tercer año, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de los equipos appliance antispam. También deberá adjuntar reportes con el siguiente contenido: Eventos, alertas, estado de salud del hardware.

- El plazo para la entrega del informe será de hasta siete (07) días calendario, contabilizados a partir del día siguiente de haber concluido cada mantenimiento preventivo

La presentación de cada entregable será dirigido a la Oficina General de Tecnología de la Información y debe ser presentados a través de Mesa de Partes Virtual mediante el enlace: <https://mpv.mtc.gob.pe/> o de forma física en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos N° 1203 – Cercado de Lima, previa reservas de citas en línea a través de: <https://citas.mtc.gob.pe>, de lunes a viernes en el horario de 8:30 horas a 17:30 horas, siendo que los remitidos fuera de esa hora serán recepcionados como si hubiesen sido entregados al día siguiente hábil.

9 REQUISITOS Y RECURSOS DEL POSTOR

9.1 REQUISITOS DEL POSTOR

- El postor debe ser representante autorizado o partner autorizado en el Perú, de los equipos ofertados, para lo cual deberá presentar carta del fabricante que lo acredite como representante autorizado o partner autorizado para comercializar y brindar los servicios de configuración, instalación y soporte. Dicho documento deberá ser presentado para la suscripción del contrato.
- Cada equipo debe ser nuevo, de primer uso, debe ser el último modelo disponible o liberado por el fabricante y de fabricación no anterior al año 2022, lo cual será acreditado a la entrega de los equipos mediante una carta o documento del fabricante que confirme le fecha de fabricación de los equipos antisipam.

9.2 RECURSOS DEL POSTOR

9.2.1 DEL PERSONAL CLAVE

a) JEFE DE PROYECTO

i) Actividades

Un (01) Jefe de Proyecto, que será el responsable de la coordinación y gestión durante toda la etapa de instalación y puesta en funcionamiento de los equipos appliance antisipam.

✓ Formación académica:

- Mínimo Bachiller en la carrera de Ingeniería de Sistemas, o Ingeniería de Sistemas y Computo, o Ingeniería de Computación o Ingeniería Electrónica, o Ingeniería Informática, o Ingeniería de Sistemas Empresariales, o Ingeniería industrial, o Ingeniería de Sistemas y Computación, o Ingeniería Empresarial y de Sistemas.¹⁴
- Debe contar con certificación vigente en Project Management Professional (PMP) o diplomado de especialización en dirección y gestión de proyectos o Diplomado en Gestión de Proyectos con base en el enfoque del Project Management Institute. Para ello deberá adjuntar copia del certificado o diploma correspondiente.¹⁵

b) ESPECIALISTA EN IMPLEMENTACIÓN, SOPORTE TÉCNICO, MANTENIMIENTO

i) Actividades

Un (01) especialista que será responsable de la instalación, soporte técnico y mantenimiento de los equipos appliance antisipam.

✓ Formación académica:

- Mínimo Técnico Titulado en la carrera técnica de Electrónica y Telecomunicaciones, o Computación y Sistemas, o Computación e Informática de Sistemas, o Sistemas Empresariales, Informática y Sistemas, o Sistemas de Información, o Sistemas e Informática, Redes

¹⁴ Consulta (54) del pliego de consultas presentada por el participante AGGITY PERU S.A.C.

¹⁵ Consulta (58) del pliego de consultas presentada por el participante LOTENGO PERU S.A.C.

y Comunicaciones, o Sistemas, Cómputo y Telecomunicaciones, o Sistemas y Computación o Cómputo y/o Redes y Comunicaciones de Datos o Telecomunicaciones o Sistemas y Computación o Sistemas o Electrónica o Redes y comunicaciones o Ingeniería de Seguridad y Auditoría Informática o Cómputo y Telecomunicaciones o redes o informática o sistemas.¹⁶

- Deberá contar con una certificación técnica emitida por el fabricante en función a la solución ofertada o a la ciberseguridad, considerando como mínimo la denominación Network Security Profesional o Network Security Specialist o Network Security Architech o Network Security Administrator o Network Security System. Para ello deberá adjuntar copia del certificado.¹⁷

Nota: Las certificaciones y los grados o títulos deberán ser presentados como parte de la documentación para perfeccionar el contrato.

10 **FORMA DE PAGO**

La entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendarios siguientes de otorgada la conformidad correspondiente, según lo indicado a continuación:

a) **PRESTACIÓN PRINCIPAL**

Único pago: El pago se efectuará en moneda nacional, en único pago correspondiente al 100% del monto total ofertado de la prestación principal. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, el Entidad debe contar con la siguiente documentación:

- Recepción de los bienes por parte del almacén central del MTC.
- Comprobante de pago.
- Entregables indicados en el numeral 8.1

b) **PRESTACIÓN ACCESORIA**

La prestación accesoria tendrá el siguiente esquema de pago:

✓ **Sobre el mantenimiento preventivo y soporte técnico.**

Para cada una de las prestaciones accesorias, referidas al mantenimiento preventivo y soporte técnico, el pago se efectuará en moneda nacional, en tres pagos parciales, conforme al siguiente detalle:

Primer pago: 33% del monto total ofertado por tipo de prestación accesoria, según corresponda, al finalizar los trescientos sesenta y cinco (365) días calendario de iniciada la prestación accesoria, luego de la presentación del Entregable N° 01 de la prestación accesoria correspondiente y previa conformidad otorgada por la Oficina de Infraestructura Tecnológica y Seguridad Informática.

Segundo pago: 33% del monto total ofertado por el tipo de prestación accesoria, según corresponda, al finalizar los setecientos treinta (730) días calendario de iniciada la prestación accesoria correspondiente, luego de la presentación del Entregable N° 02 de la prestación accesoria correspondiente y previa conformidad otorgada por la Oficina de Infraestructura Tecnológica y Seguridad Informática.

Tercer pago: 34% del monto total ofertado por el tipo de prestación accesoria, según corresponda, al finalizar los mil noventa y cinco (1095) días calendario de iniciada la prestación accesoria correspondiente, luego de la presentación del Entregable N°

¹⁶ Consulta (34) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.
Consulta (55) del pliego de consultas presentada por el participante AGGITY PERU S.A.C.

Consulta (60) del pliego de consultas presentada por el participante LOTENGO PERU S.A.C

¹⁷ Consulta (35) del pliego de consultas presentada por el participante TELEFONICA DEL PERU S.A.A.
Consulta (62) del pliego de consultas presentada por el participante LOTENGO PERU S.A.C.

03 de la prestación accesoria correspondiente y previa conformidad otorgada por la Oficina de Infraestructura Tecnológica y Seguridad Informática.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- ✓ Informe de conformidad de la Oficina de Infraestructura Tecnológica y Seguridad Informática correspondiente a la prestación efectuada por el contratista.
- ✓ Comprobante de pago.
- ✓ Presentación de los entregables indicados en el numeral 8.2.2 y 8.2.3

✓ **Sobre la capacitación**

El pago se efectuará en moneda nacional, en único pago correspondiente al 100% del monto total ofertado para la capacitación, previa presentación de los certificados de cada uno de los participantes.

Dicha documentación se debe presentar en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos N° 1203 –Cercado de Lima, en el horario de 8:30 horas a 17:30 horas, previa reservas de citas en línea a través de: <https://citas.mtc.gob.pe> o a través de Mesa de Partes Virtual del MTC, accediendo desde el siguiente link: <https://mpv.mtc.gob.pe>.

11 **PENALIDADES**

11.1 **PENALIDADES POR MORA**

En la ejecución de la adquisición de los bienes, se aplicarán las penalidades por mora de acuerdo a lo establecido en los artículos 161° y 162° del Reglamento de la Ley de Contrataciones del Estado.

Si el contratista 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 = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el Contratista acredite de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de la Entidad no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

11.2 **OTRAS PENALIDADES**

De acuerdo con el artículo 163 del Reglamento se considerarán además las siguientes penalidades:

N°	Supuestos de aplicación de penalidad	Procedimiento	Forma de cálculo
01	Por no prestar el servicio de soporte técnico o atención a consultas técnicas en un tiempo máximo de cuatro (4) horas.	Tiempo empleado por el CONTRATISTA para brindar una atención que no implique un incidente con los equipos de seguridad de correo electrónico. El tiempo se contabiliza desde la comunicación por parte de la entidad, el mismo se acreditará con el código de avería o de registro y/o correo electrónico. La penalidad aplica por demora en los diferentes niveles de atención de los requerimientos y/o incidentes, en donde el Director General de la Oficina General de Tecnología de la Información notificará a través de un documento a la Oficina de	1% del valor de una (01) UIT por ocurrencia.

N°	Supuestos de aplicación de penalidad	Procedimiento	Forma de cálculo
		Abastecimiento el no cumplimiento para la aplicación de la penalidad. ¹⁸	
02	Por exceder el tiempo de presentación de los entregables (prestación accesoria).	Tiempo empleado por el CONTRATISTA para realizar la presentación de los entregables correspondientes a las prestaciones accesorias de acuerdo a lo precisado en el ítem 8.2.2 y 8.2.3. La penalidad aplica por demora en los diferentes niveles de atención de los requerimientos y/o incidentes, en donde el Director General de la Oficina General de Tecnología de la Información notificará a través de un documento a la Oficina de Abastecimiento el no cumplimiento para la aplicación de la penalidad.	1% del valor de una (01) UIT día de retraso
03	Por exceder el tiempo de resolución de incidentes, cuyo tiempo máximo es de veinticuatro (24) horas.	Tiempo empleado por el CONTRATISTA para brindar el soporte correctivo y resolver el incidente reportado. El tiempo se contabiliza desde que genera el ticket de atención al MTC. La penalidad aplica por demora en los diferentes niveles de atención de los requerimientos y/o incidentes, en donde el Director General de la Oficina General de Tecnología de la Información notificará a través de un documento a la Oficina de Abastecimiento el no cumplimiento para la aplicación de la penalidad. Nota: El CONTRATISTA deberá informar mediante correo electrónico el código del ticket del incidente reportado.	3% del valor de una (01) UIT por ocurrencia.
04	Por exceder el tiempo de solución a errores (bug) propios de los equipos, cuyo tiempo máximo de resolución es setenta y dos (72) horas.	En caso que el incidente no pueda ser resuelto vía mesa de ayuda y el Contratista deba escalarlo directamente al fabricante Asimismo, deberá cumplirse para casos en donde se pierda la gestión total de la consola de administración o en casos de daño del sistema operativo base de los equipos. La penalidad aplica por demora en los diferentes niveles de atención de los requerimientos y/o incidentes, en donde el Director General de la Oficina General de Tecnología de la Información notificará a través de un documento a la Oficina de Abastecimiento el no cumplimiento para la aplicación de la penalidad.	5% del valor de una (01) UIT por ocurrencia.

UIT: Unidad Impositiva Tributaria.

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

12 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

12.1 ÁREA QUE COORDINARÁ CON EL CONTRATISTA

El área que coordinará con el contratista es la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.

12.2 ÁREA QUE BRINDARÁ LA RECEPCIÓN Y CONFORMIDAD RECEPCIÓN DE BIENES

La recepción de los bienes será en el almacén central del MTC, debiendo contar con la presencia de un representante de Almacén Central, un representante de la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información y un representante del CONTRATISTA.

¹⁸ [Consulta \(5\) del pliego de consultas presentada por el participante SSG PERU S.A.C.](#)

CONFORMIDAD:**DE LA PRESTACION PRINCIPAL:**

La conformidad de la prestación principal será otorgada por la Oficina General de Administración, en su calidad de Unidad Ejecutora de Inversiones, previo informe técnico de validación y cumplimiento con las especificaciones técnicas de la recepción de los equipos; emitido por la Oficina de Infraestructura Tecnológica y Seguridad de la Información (OITSI) de la Oficina General de Tecnología de la Información (OGTI) del Ministerio de Transportes y Comunicaciones (MTC) adjuntando el documento de ingreso e recepción de bienes al almacén central".

DE LAS PRESTACIONES ACCESORIAS:**- Sobre el mantenimiento preventivo y soporte técnico:**

La conformidad será emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática, en un plazo de siete (07) días calendario luego de realizado cada mantenimiento preventivo y soporte técnico en el periodo correspondiente, y previa presentación del entregable correspondiente al mantenimiento preventivo y soporte técnico indicado en el numeral 8.2.2 y 8.2.3

- Sobre la capacitación

La conformidad será emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática, en un plazo de siete (07) días calendario luego de presentado los certificados correspondientes a la capacitación.

13 CONFIDENCIALIDAD

Toda información del MTC a que tenga acceso el CONTRATISTA, producto del desarrollo de la prestación contratada es estrictamente confidencial. El CONTRATISTA y su personal, deben comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito de la Oficina General de Tecnología de la Información.

El Contratista deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida revelarla a terceros.

14 RESPONSABILIDAD POR VICIOS OCULTOS

El CONTRATISTA es responsable por la cantidad ofrecida y por los vicios ocultos de los bienes y servicios ofertados por un plazo máximo de tres (03) años, contados a partir del día siguiente de la conformidad emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática.

15 SUBCONTRATACIÓN

No aplica.

16 NORMAS ANTICORRUPCIÓN

El contratista acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anti-corrupción. Sin limitar lo anterior, el contratista se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anti-corrupción, sin restricción alguna.

En forma especial, el contratista declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

17 **NORMAS ANTISOBORNO**

El contratista no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que puedan constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderado, representantes legales, funcionarios, asesores o personas vinculadas.

Asimismo, el contratista se obliga a conducirse en todo momento, durante la ejecución del contrato. Con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en el artículo 11º de la Ley de Contrataciones del Estado y el artículo 7º de su Reglamento.

Asimismo, el contratista se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por el MTC.

De la misma manera, el contratista es consciente que de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que el MTC pueda accionar.

18 **CUMPLIMIENTO DE PROTOCOLOS SANITARIOS**

El Contratista se compromete a cumplir con las disposiciones para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a "SARS-CoV-2", por el periodo de vigencia establecido por las autoridades competentes.

19 **REQUISITOS DE CALIFICACIÓN**

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 800,000.00 (ochocientos mil con 00/100 soles) por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none">- Venta de licencias y equipos o sistemas de control y seguridad de correo (Antispam) o- venta de licencias y equipos de filtro de contenido Web (Proxy Web o Web Filter) o- venta de licencias y equipos IPS. <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p>



	<p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>Importante: <i>En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".</i></p>
B	CAPACIDAD TÉCNICA Y PROFESIONAL
	EXPERIENCIA DEL PERSONAL CLAVE
	<p>Requisitos: <u>Un (01) Jefe de proyecto.</u> Con experiencia mínima de cinco (05) años en la jefatura de proyectos de soluciones de seguridad antispam o soluciones corporativas de software de protección de puntos finales o servidores como Firewall de Próxima Generación o Filtro de Contenido Web o soluciones de seguridad informática.¹⁹</p> <p><u>Un (01) especialista en implementación, soporte técnico y mantenimiento:</u> Con experiencia mínima de tres (03) años en la instalación o configuración o soporte técnico de soluciones de seguridad antispam o soluciones corporativas de software de protección de puntos finales y/o servidores como Firewall de Próxima Generación o Filtro de Contenido Web.</p> <p>Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>Importante: •El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores. •Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento. •En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. •Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años</p>

¹⁹ Consulta (28) del pliego de consultas presentada por el participante TELEFÓNICA DEL PERÚ S.A.A.





PERÚ

Ministerio
de Transportes
y Comunicaciones

Secretaría General

Oficina General de
Tecnología de la
Información

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

	<i>anteriores a la fecha de la presentación de ofertas.</i>
--	---

