



REQUERIMIENTO PARA LA CONTRATACIÓN DE SERVICIOS

1	ÁREA USUARIA	Unidad de Infraestructura y Soporte Tecnológico												
2	DENOMINACIÓN DE LA CONTRATACIÓN	SERVICIO DE MANTENIMIENTO PREVENTIVO Y SOPORTE TÉCNICO DE LA SOLUCIÓN FILTRO DE CONTENIDO WEB DE LA MARCA FORCEPOINT O EQUIVALENTE												
3	FINALIDAD PÚBLICA DE LA CONTRATACIÓN	La contratación tiene por finalidad el buen desempeño y calidad de nuestra red del servicio de Internet en los usuarios; asimismo, se requiere minimizar el tiempo infructífero de los usuarios con acceso al servicio de Internet y minimizar el riesgo de infecciones por malware en las PC's de nuestra red; garantizando además la disponibilidad, confidencialidad, integridad y la calidad de los servicios de la información que administra el RENIEC.												
4	OBJETIVO GENERAL DE LA CONTRATACIÓN	Contratar a una persona natural o jurídica que brinde el Servicio de mantenimiento preventivo y Soporte técnico de la solución filtro de contenido web de la marca Forcepoint o equivalente.												
5	ALCANCES Y ACTIVIDADES A DESARROLLAR	<p>A. CONSIDERACIONES GENERALES:</p> <p>Mediante Resolución de Oficina N° 000450-2023/OAF/RENIEC se aprueba la estandarización para el servicio de Mantenimiento Preventivo y Soporte Técnico de la solución filtro de contenido Web de la marca Forcepoint.</p> <p>El contratista debe brindar la renovación del Servicio de soporte, mantenimiento, actualización de garantía y suscripción de la solución "Filtro de Contenido (FORCEPOINT)", permitiendo la actualización permanente de la plataforma a las futuras versiones del producto preexistente durante el plazo de ejecución de la prestación indicada en el 7.4 de los términos de referencia, garantizando adicionalmente su operatividad en caso de averías.</p> <p>El servicio está conformado por lo siguiente:</p> <p>A. 1 MANTENIMIENTO PREVENTIVO.</p> <p>El contratista debe realizar los mantenimientos preventivos, durante el plazo de ejecución de la prestación indicada en el 7.4 de los términos de referencia.</p> <ul style="list-style-type: none">Los mantenimientos preventivos serán de acuerdo al siguiente cuadro, contabilizado a partir del inicio del servicio; para el inicio de servicio se suscribirá un ACTA DE INICIO DEL SERVICIO por parte de la Unidad de Infraestructura y Soporte Tecnológico (UIST): <table><thead><tr><th>N°</th><th>Descripción</th><th>Periodo</th></tr></thead><tbody><tr><td>1</td><td>Primer mantenimiento preventivo</td><td>Mes 8</td></tr><tr><td>2</td><td>Segundo mantenimiento preventivo</td><td>Mes 16</td></tr><tr><td>3</td><td>Tercer mantenimiento preventivo</td><td>Mes 24</td></tr></tbody></table> <p>Los horarios y fechas de los mantenimientos preventivos serán coordinados previamente entre el contratista y el personal del área de</p>	N°	Descripción	Periodo	1	Primer mantenimiento preventivo	Mes 8	2	Segundo mantenimiento preventivo	Mes 16	3	Tercer mantenimiento preventivo	Mes 24
N°	Descripción	Periodo												
1	Primer mantenimiento preventivo	Mes 8												
2	Segundo mantenimiento preventivo	Mes 16												
3	Tercer mantenimiento preventivo	Mes 24												



seguridad de la Unidad de Infraestructura y Soporte Tecnológico (UIST) del RENIEC, en la reunión de Kick Off que se realizará a los dos (02) días calendario siguientes de firmado el Contrato.

El mantenimiento preventivo consistirá como mínimo de lo siguiente:

- Diagnóstico del hardware y plataforma base.
- Licenciamiento del hardware preexistente que soportará 5000 usuarios
- Optimización de las políticas de seguridad.
- Limpieza externa e interna del hardware.
- Otras actividades esenciales para poner en funcionamiento el servicio y alcanzar la finalidad pública de la contratación; considerándose que el servicio es a todo costo.

El contratista debe brindar licenciamiento que permita usar la solución OnPremise y/o Forcepoint Web Security durante el plazo de ejecución de la prestación. Este licenciamiento deberá permitir como mínimo lo siguiente:

CARACTERISTICAS GENERALES	
Arquitectura	<ul style="list-style-type: none"> • La solución debe tener una sola consola de administración para Security Web Gateway, CASB y ZTNA. • La solución debe tener un único agente unificado para Security Web Gateway, CASB y ZTNA. • La solución debe ser compatible con cualquier aplicación HTTP(S) desde cualquier dispositivo sin un agente. • La solución debe admitir un tiempo de actividad del 99,99 %. • La solución debe soportar más de 300 PoP (Puntos de Presencia). • La solución debe ser compatible con el control de acceso contextual. • La solución debe contar con escalabilidad flexible. • La solución de filtro de contenido web deberá ser en la nube.
Cumplimiento y Certificaciones	<ul style="list-style-type: none"> • La solución debe tener la certificación SOC-2 Tipo 2. • La solución debe tener las certificaciones ISO27001, ISO27017 e ISO27018. • La solución debe tener la certificación FedRamp. • La solución debe tener un estado en tiempo real del servicio.
Integraciones	<ul style="list-style-type: none"> • La solución debe tener soporte IPsec universal. • La solución debe tener Soporte Universal GRE. • La solución debe tener soporte para planos de datos redundantes. • La solución debe admitir la integración con cualquier IdP compatible con SAML. • La solución debe ser compatible con Active Directory mediante agente de sincronización. • Admite el envío de datos de amenazas a un SIEM a través de una fuente de syslog. • La solución debe tener capacidad de exportación de registros a SIEM de terceros.





			<ul style="list-style-type: none">• La solución debe integrarse con los proveedores de identidad para dirigir el tráfico a través del proxy en línea después de la autenticación.• La solución debe admitir la integración con soluciones MDM/EMM para compilar una lista de identificadores únicos de dispositivos
		Registro y alertas	<ul style="list-style-type: none">• La solución debe admitir el filtrado de infracciones en función de múltiples dimensiones (por ejemplo, usuario, política, patrón de datos, intervalo de fechas.)• La solución debe admitir la clasificación de infracciones en función de los encabezados de las columnas (por ejemplo, gravedad, política, estado, fecha.)• La solución debe proporcionar el número de infracciones desencadenadas en el documento u objeto, el usuario y la actividad.• La solución debe proporcionar extractos que desencadenaron la infracción con contenido coincidente resaltado• La solución debe admitir el marcado de infracciones con un estado (por ejemplo, falso positivo, nuevo, abierto, resuelto)
		Monitoreo histórico y en tiempo real	<ul style="list-style-type: none">• La solución debe admitir la capacidad de filtrar según el tipo de actividad o las últimas semanas y días• La solución debe admitir la capacidad de escribir parámetros de filtrado en una barra de búsqueda/filtro para orientar actividades específicas, usuarios.• La solución debe admitir actividades de filtrado basadas en un intervalo de fechas específico o número de días/meses anteriores.
		Administración	<ul style="list-style-type: none">• La solución debe ser compatible con MFA o Admin Portal Access• La solución debe ser compatible con el control de acceso basado en roles (RBAC)• La solución debe admitir una función de administrador para crear y editar políticas• Los soportes deben admitir un rol de administrador para configurar la aplicación, los usuarios y las alertas.• La solución debe admitir diferentes vistas que se adapten a la medida de las personas y los casos de uso específicos de los usuarios.
		Gestión de identidad	<ul style="list-style-type: none">• La solución debe ser compatible con la funcionalidad de inicio de sesión single sign-on.• La solución debe ser compatible con capacidades IdP/IAM integradas en caso de que no haya una solución IDP/IAM disponible.• La solución debe admitir la autenticación multifactor en las aplicaciones en la nube como mecanismo de mitigación de riesgos.• La solución debe admitir la integración con Active Directory y Azure AD para la autenticación de usuarios y la sincronización de unidades organizativas/grupos de seguridad.• La solución debe ser compatible con la integración con cualquier solución de administración de identidades para autenticar el acceso a los servicios en la nube sancionados.
		Notificaciones	<ul style="list-style-type: none">• La solución debe admitir el envío de un correo electrónico al usuario final cuando se activa una política.



			<ul style="list-style-type: none"> • La solución debe admitir el envío de un correo electrónico a un administrador cuando se activa una política. • La solución debe admitir la creación de un incidente/alerta cuando se activa una política.
		Control de acceso contextual	<ul style="list-style-type: none"> • La solución debe permitir el acceso a los dispositivos administrados • La solución debe admitir el bloqueo del acceso a dispositivos no administrados • La solución debe admitir el bloqueo del acceso a aplicaciones no autorizadas • La solución debe admitir políticas basadas en departamento, geolocalización, dispositivo y otros atributos • La solución debe permitir que los dispositivos personales vean contenido en línea, pero no lo descarguen o carguen • La solución debe admitir la identificación del dispositivo administrado mediante el uso de un agente • La solución debe admitir la identificación del dispositivo administrado mediante un certificado de cliente • La solución debe admitir la identificación del dispositivo administrado por un atributo SAML • La solución debe admitir el bloqueo de registros desde ubicaciones o dispositivos de riesgo • La solución debe admitir el retraso en el inicio de sesión en función de un comportamiento de riesgo • La solución debe admitir la configuración de un tiempo de inactividad personalizado antes de aplicar la reautenticación • La solución debe admitir la activación de MFA según el grupo, el dispositivo, la ubicación, el comportamiento, el intervalo de tiempo o cualquier combinación de criterios.
		Eventos	<ul style="list-style-type: none"> • Admite el filtrado de infracciones en función de múltiples dimensiones (por ejemplo, usuario, política, patrón de datos, rango de fechas) • Admite la clasificación de infracciones según los encabezados de las columnas (por ejemplo, gravedad, política, estado, fecha) • Proporciona el número de infracciones desencadenadas en el documento u objeto, el usuario y la actividad.
		Análisis y Control de Geolocalización	<ul style="list-style-type: none"> • La solución debe admitir la detección y el bloqueo de inicios de sesión de países no autorizados • La solución debe admitir la detección de inicios de sesión simultáneos desde ubicaciones geográficamente distantes • La solución debe admitir la creación de ubicaciones personalizadas para identificar los sitios de los clientes
		Funcionalidades forenses	<ul style="list-style-type: none"> • La solución debe admitir la capacidad de filtrar la pista de auditoría para un usuario específico al período de tiempo que rodea el incidente. • La solución debe admitir la capacidad de ver una fuente de actividad para un usuario específico.
		Funcionalidad de Filtro Web	<ul style="list-style-type: none"> • La solución debe ser compatible y contar con una aplicación de punto final. • La solución debe ser compatible con Forward Proxy.



		<ul style="list-style-type: none"> • La solución debe hacer cumplir políticas de uso aceptable. • La solución debe admitir categorías de URL basadas en la reputación. • La solución debe controlar el acceso hasta el nivel de ruta o path del directorio de la URL. • La solución debe admitir categorías de URL personalizadas. • La solución debe admitir el descifrado TLS según la categoría de URL. • La solución debe bloquear la carga de datos sensibles a cualquier sitio web. • La solución debe ser compatible con Anti-Malware. • La solución debe bloquear la descarga de malware desde cualquier sitio web. • La solución debe ser compatible con funcionalidades de descarga de DLP. • Debe permitir aplicar política a redes de invitados. • La solución debe permitir aplicar políticas usando librerías para PII, PHI y PCI. • La solución debe ser compatible con funcionalidades de carga de DLP.
	Aislamiento de navegador remoto (RBI)	<ul style="list-style-type: none"> • La solución debe ser compatible con Frame Streaming (Transmisión segura) • La solución debe ser compatible con DOM Rendering (Secure Rendering) • La solución debe ser compatible con Smart Rendering • La solución debe ser compatible con Zero Trust CDR • La solución debe ser compatible con la protección esteganográfica ZT-CDR • La solución debe ser compatible con la entrada de teclado en chino tradicional/simplificado • La solución debe ser compatible con Solo lectura y Navegación segura • La solución debe admitir navegadores móviles
	Shadow IT	<ul style="list-style-type: none"> • La solución debe admitir el descubrimiento y la clasificación automáticos de cientos de miles de aplicaciones en la nube no autorizadas • La solución puede descubrir el uso de aplicaciones SaaS en la nube autorizadas y no autorizadas en el panel empresarial de SWG.

B. SOPORTE TÉCNICO.

El Soporte técnico (24x7x365), garantía de la solución y versión de producto; para el caso de averías, incidencias, configuraciones y/o consultas técnicas, incluyendo el soporte in site o remoto.

Las asignaciones de tickets por las solicitudes o incidentes reportadas por el RENIEC, no deben exceder los 15 minutos, contados a partir de la remisión y/o notificación del incidente por parte de la Unidad de Infraestructura y Soporte Tecnológico, quiere decir que dentro de este periodo de tiempo se debe generar el ticket correspondiente, las resoluciones de las solicitudes y/o incidentes críticos o altos no deben exceder de las 2 horas, contados a partir de la generación del tickets, las resoluciones de solicitudes y/o incidentes medios o moderados no deben exceder de las 4 horas, contados a partir de la generación del tickets y las resoluciones para las solicitudes y/o incidentes



bajos no deben exceder de las 8 horas, contados a partir de la generación del tickets.

Nivel de soporte	Tipo de Asistencia	Tiempo máximo de respuesta
Crítico o alto	In site/Asistencia remota	2 horas
Medio o moderado	In site/Asistencia remota/email	4 horas
Bajo	Asistencia Remota/email/Teléfono	8 horas

- **Crítico o Alto:** Impacto grave, muy alto o catastrófico al servicio, ocasionando pérdida de imagen Institucional y/o ocasionando graves pérdidas económicas.
- **Medio o Moderado:** Impacto leve, medio o moderado al servicio, ocasionando incumplimiento de ANS y/o pérdidas económicas importantes y moderadas.
- **Bajo:** Impacto bajo o muy bajo al servicio, ocasionando pérdidas económicas bajas.

Administración y Seguridad gestionada incluyendo el monitoreo, la gestión de eventos y atención de tickets

La solución debe permitir la administración y seguridad gestionada incluyendo el monitoreo, la gestión de eventos y atención de tickets que tendrán las siguientes características:

ADMINISTRACIÓN Y SEGURIDAD GESTIONADA INCLUYENDO EL MONITOREO	
Configuración y Mantenimiento de Forcepoint Web Security Light	<ul style="list-style-type: none"> • Administración y configuración de políticas de seguridad específicas para Forcepoint Web Security Light. • Actualización y ajuste periódico de las políticas de seguridad para reflejar las necesidades cambiantes
Integración y Monitoreo	<ul style="list-style-type: none"> • Integración de Forcepoint Web Security Light con otras herramientas de seguridad y sistemas de monitoreo para una visibilidad completa de los eventos de seguridad.
Detección y Respuesta	<ul style="list-style-type: none"> • Monitoreo constante de eventos de seguridad en Forcepoint Web Security Light para detectar actividades inusuales o sospechosas. • Configuración de alertas y notificaciones para eventos significativos
Gestión de Incidentes de Seguridad	<ul style="list-style-type: none"> • Recepción y clasificación de tickets de seguridad relacionados con Forcepoint Web Security Light. • Seguimiento y documentación de las acciones tomadas para resolver los incidentes.
Actualizaciones y Parches	<ul style="list-style-type: none"> • Gestión de actualizaciones y parches de Forcepoint Web Security Light para mantener la solución segura y actualizada



Informe y Análisis	• Generación mensualizada de informes periódicos de seguridad y análisis de tendencias para evaluar la efectividad de las políticas de seguridad
Actualizaciones y Parches	• Gestión de actualizaciones y parches de Forcepoint para mantener el equipo seguro y actualizado
GESTIÓN DE EVENTOS DE ATENCIÓN DE TICKETS	
Gestión de Incidentes y Tickets	<ul style="list-style-type: none"> • Monitoreo y gestión de tickets de seguridad, incluyendo la recepción, clasificación y asignación de incidentes. • Seguimiento y documentación exhaustiva de la resolución de tickets
Priorización de Tickets	• Establecimiento de un proceso de priorización para tickets de seguridad en función de la gravedad, el impacto y la urgencia
Comunicación con el Cliente	• Comunicación proactiva con RENIEC para informar sobre el estado de los incidentes, las acciones tomadas y las recomendaciones de seguridad
Informe de Incidentes	• Generación de informes detallados de incidentes y actividades realizadas para RENIEC
Capacitación del Cliente	• Proporcionar capacitación a RENIEC sobre buenas prácticas de seguridad y cómo reportar incidentes de seguridad de manera efectiva
Revisión y Mejora Continua	• Realización de revisiones periódicas con RENIEC para evaluar el desempeño del servicio y realizar mejoras continuas

B.1 SUSCRIPCIÓN

- **Alcance de la Suscripción:** La suscripción requerida debe tener una capacidad de atender cinco mil (5000) usuarios.
- El contratista es responsable durante la ejecución de la prestación contra defectos de diseño y/o fabricación, averías o fallas de funcionamiento de la solución preexistentes.
El fabricante debe brindar un 99.99% de disponibilidad del servicio de la solución contratada.
- El contratista debe presentar dentro de los 60 días siguientes de la suscripción del contrato, la documentación de las condiciones de garantía por parte del fabricante de los equipos preexistentes, por el plazo de ejecución del servicio contado a partir del inicio del servicio, en el cual se indiquen los SLA. El SLA mínimo aceptable será del 99.99% de disponibilidad.

La solución deberá contar con actualizaciones que deben ser aplicadas automáticamente, y estas no deben estar en etapa de obsolescencia o que se haya anunciado su "End-of-Life" y/o fin de soporte por parte del fabricante.

Características de la Suscripción para el soporte de hardware preexistente: Debe incluir las siguientes características:

- Apertura del caso por medio del postor o directamente por la entidad.



- Acceso al TAC del fabricante en horario 24x7.
- No se debe requerir un triaje para abrir un caso.
- Tiempo de respuesta para la más alta severidad de 30 minutos.
- Los ingenieros asignados como punto principal de contacto deben ser responsables de resolver los problemas de la solución ofertada, para los siguientes escenarios: producto único, múltiples productos y/o múltiples fabricantes.
- Los expertos deben coordinar la resolución de problemas con otros fabricantes si es necesario, para aquellos fabricantes que tengan una alianza con el fabricante de la solución atendida.
- Debe incluir la capacidad de observar más allá del alcance del caso original y recomendar acciones para abordar problemas conocidos.
- Los ingenieros asignados deben tener amplia experiencia en soluciones, arquitecturas e interoperabilidad entre software y hardware del fabricante de la solución atendida.

5.1 ACTIVIDADES

- a) Reunión de KickOff, que se realizará a los dos (02) días calendario siguientes de firmado el contrato. El contratista presentará a su personal responsable del servicio solicitado.
- b) El contratista realizará las Visitas técnicas a las instalaciones del RENIEC, Centro de Datos "Housing" y Centro de Datos "San Borja", El cronograma de visitas será definidas en la reunión de KickOff.

5.2 PLAN DE TRABAJO DEL SERVICIO

Dentro de los cinco (5) días calendario siguientes a la suscripción del contrato, el Contratista debe entregar un Plan de Trabajo del Servicio, el cual debe contener el detalle de las actividades de implementación; además, debe incluir como mínimo los siguientes rubros:

- a. Descripción de la arquitectura/topología.
 - b. Mejoramiento de las políticas pre existentes.
 - c. Cronograma de los mantenimientos preventivos.
 - d. Protocolo de pruebas de cada una de las políticas implementadas.
- El protocolo de pruebas propuesto será validado por el RENIEC conjuntamente con el Contratista.

El Plan de Trabajo del Servicio será aprobado y/u observado por parte de la Unidad de Infraestructura y Soporte Tecnológico, dentro de los dos (2) días de recibido el plan de trabajo.

IMPLEMENTACIÓN

- Diagnóstico del hardware y plataforma base
- Licenciamiento del hardware preexistente que soportará 5000 usuarios
- Optimización de las políticas de seguridad.
- Limpieza externa e interna del hardware

5.3 INICIO DEL SERVICIO

El inicio del servicio se contará a partir del día siguiente de la suscripción del ACTA DE INICIO DEL SERVICIO y al finalizar el Contrato vigente.



Al culminar la etapa de implementación, se debe emitir el Acta de Conformidad por la Implementación del servicio, que será suscrita por el Contratista y la Unidad de Infraestructura y Soporte Tecnológico del RENIEC.

El contratista dentro de los tres (3) días calendario posteriores a la implementación total del servicio, el Contratista debe entregar por Mesa de Partes un INFORME FINAL DE LA IMPLEMENTACIÓN en formato digital (PDF), donde se detallen el servicio implementado, que contenga por lo menos lo siguiente:

- a. Descripción de la arquitectura y diagrama de la Topología de la red.
- b. Listado de configuración y mejoramiento de las políticas pre existente.
- c. Registros de protocolos de pruebas
- d. Información de contactos para el reporte, atención de averías y escalamiento de solicitudes para el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), el cual debe incluir como mínimo: Teléfonos, correo electrónico y página web.
- e. Procedimiento e información de contacto para solicitudes al área comercial, el cual debe incluir como mínimo: Teléfono y correo electrónico.

5.4 RECURSOS A SER PROVISTOS POR EL CONTRATISTA

Todos los equipos, materiales y accesorios necesarios para la continuidad y ejecución del servicio, será responsabilidad del Contratista.

Será de total y exclusiva responsabilidad del Contratista contemplar todas las actividades, dispositivos, componentes, suscripciones y accesorios para la correcta ejecución de los componentes para continuar con el servicio requerido en los plazos mencionados.

El Contratista será responsable de las siguientes actividades requeridas para el suministro del servicio:

- ✓ Pruebas de funcionamiento y aceptación según protocolo.
- ✓ Puesta en servicio.
- ✓ Supervisión permanente de los acuerdos de niveles de servicio (ANS).
- ✓ Otras actividades inherentes a la provisión del servicio, es decir cualquier otra actividad no específicamente detallada en los términos de referencia y que sea necesaria para dejar operativo el servicio.

5.5 RECURSOS A SER PROVISTOS POR LA ENTIDAD

El RENIEC brindará todas las facilidades de acceso a sus oficinas al personal del Contratista del servicio. Es responsabilidad del Contratista la gestión de permisos, autorizaciones y suscripciones para los trabajos que tengan que realizar en espacios que no son propiedad del RENIEC y de existir gastos relacionados al mismo, estos deberán ser asumidos por el Contratista.

5.6 REQUERIMIENTOS DEL CONTRATISTA Y DE SU PERSONAL

No estar inhabilitado para contratar con el estado peruano.



El Contratista deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas para reportes de fallas, centros de gestión, y personal de reparación de averías. Asimismo, deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten.

El Contratista debe asegurar y garantizar al RENIEC, que toda la infraestructura tecnológica implementada y/o instalada para la prestación del servicio, se encuentren correctamente activas y licenciadas que cumplan con los acuerdos de los niveles de servicio y términos de referencia establecidos, debiéndose acreditar tal compromiso en el primer "Informe de Servicio", adjuntando la documentación respectiva (suscripciones y/o cartas de soporte de fabricantes).

Actividades del personal clave:

Jefe del Proyecto

(Cantidad: 01)

1. Responsable de planificar el mantenimiento y soporte de la solución de filtro de contenido web. Esto incluye la programación de actividades, la asignación de recursos y la definición de objetivos.
2. Coordinar las actividades del equipo de implementación y monitoreo. Se asegura de que todos estén informados y alineados con los objetivos y plazos del proyecto.
3. Realiza un seguimiento constante del avance del proyecto, asegurándose de que se cumplan los plazos y que se alcancen los objetivos.

Especialista de soporte técnico

(Cantidad: 01)

1. Responsable de la instalación y configuración de la solución de filtro de contenido web. Esto incluye la puesta en marcha inicial de hardware y software.
2. Personaliza la solución según los requisitos específicos de la organización, como políticas de filtrado, reglas de seguridad y políticas de acceso.
3. Realiza pruebas exhaustivas para garantizar que la solución funcione correctamente. Esto implica la detección y resolución de posibles problemas.

Especialista en Monitoreo y Seguridad Gestionada:

(Cantidad: 01)

1. Realiza un monitoreo constante de la solución de filtro de contenido web para detectar actividades inusuales, amenazas o problemas de rendimiento.
2. Responde a incidentes de seguridad o problemas operativos de la solución de filtro de contenido web. Esto puede incluir la implementación de medidas correctivas.



3. Emitir informes periódicos sobre el uso de la herramienta, las amenazas detectadas y el rendimiento de la solución.

El personal clave debe contar con la siguiente certificación:

Jefe del Proyecto

- Certificación Oficial vigente en Gestión de Proyectos
- Certificación oficial más reciente en la solución de Filtro de Contenido Web nivel administrador emitido por la marca Forcepoint.
- Certificación oficial ITIL Foundation.
- Certificación en ISO 20000 Gestión de Servicios de TI.
- Certificación en ISO 27001 Asociado a Seguridad de la Información.

Especialista de soporte técnico:

- Certificación oficial más reciente en la solución de Filtro de Contenido Web nivel administrador emitido por la marca Forcepoint.
- Certificación oficial en la solución de Filtro de Contenido emitido por la marca Forcepoint con una antigüedad no menor a cinco (05) años.
- Certificación oficial en la solución de NGFW nivel ingeniero emitido por la marca Forcepoint.
- Constancia o certificación ITIL Foundation emitida por una entidad acreditada.
- Certificación en ISO 27001 como auditor líder.
- Constancia o certificación en Ethical Hacking emitida por una entidad acreditada.
- Certificación en ISO 20000 Gestión de Servicios de TI.

Especialista en Monitoreo y Seguridad Gestionada:

- Certificación oficial en la solución de Filtro de Contenido Web nivel administrador emitido por la marca Forcepoint.
- Certificación en análisis de vulnerabilidades emitida por fabricante reconocido.
- Certificación en Information Security Operation Center – ISOC
- Certificación en Ciberseguridad Defensiva.

Las certificaciones del personal clave (**Jefe del Proyecto, Especialista de soporte técnico y Especialista en Monitoreo y Seguridad Gestionada**) se acreditará con copia simple de CONSTANCIAS, CERTIFICADOS Y/O DIPLOMA, como requisito para la suscripción del contrato.

6

**PRESTACIONES
ACCESORIAS**

6.1 Capacitación y/o entrenamiento

El contratista debe brindar capacitación en el curso oficial Forcepoint Web Security Administrator o equivalente en idioma español, para el personal de la Unidad de Infraestructura y Soporte Tecnológico.

La capacitación en la administración de la solución filtro de contenido web de la marca Forcepoint debe cumplir con los siguientes requerimientos a fin de asegurar su idoneidad técnica para el desarrollo de la solución requerido:





	<ul style="list-style-type: none">○ El centro de instrucción debe contar con los recursos necesarios para el correcto dictado del curso, como son: equipos virtuales para el desarrollo de prácticas y/o laboratorios si las hubiera en cada uno de los temas incluidos. Se aceptará que los cursos sean en modalidad virtual.○ De darse la Capacitación de manera presencial, se llevará a cabo en la sede del Centro de Instrucción elegido por el contratista.○ Los horarios para el dictado de los cursos serán definidos en coordinación con el personal de la Unidad de Infraestructura y Soporte Tecnológico del RENIEC y el Contratista, siendo preferentemente en horarios fuera de oficina.○ Capacitación con cursos a cinco (5) integrantes de la Unidad de Infraestructura y Soporte Tecnológico del RENIEC en la administración de la solución implementada, debiendo entregar los certificados de participación del curso emitido por la marca a cada participante.○ La duración del curso será como mínimo veinte (20) horas.○ Para la suscripción del contrato el postor ganador debe presentar la información relacionada a la Institución encargada de la capacitación (razón social, RUC, dirección y teléfono). Dentro de los diez (10) días calendario siguiente de la suscripción del contrato el Contratista debe acreditar la(s) certificación(es) del(los) instructor(es) en la solución implementada.○ Dictado por instructor certificado por la marca de la solución instalada.○ Dentro del plan de trabajo, el contratista debe presentar el contenido (syllabus) de los cursos, donde se mencione detalladamente los temas a tratar y el nivel que se obtendrá luego de completar estos cursos.
--	---





7	LUGAR Y PLAZO DEL SERVICIO	<p>7.1. LUGAR DE EJECUCIÓN PRESTACIÓN PRINCIPAL.</p> <p>La entrega del servicio se debe realizar en la local del Centro de Datos "Housing" dentro de Lima Metropolitana, en la Sede San Borja - Jr. Tiziano Vecellio 245 – San Borja, y en la Av. Santa Catalina 663, Santa Catalina - La Victoria Cercado de Lima, en el horario 24 x 7.</p> <p>7.2. LUGAR DE EJECUCIÓN DE LA PRESTACIÓN ACCESORIA.</p> <p>De darse la Capacitación de manera presencial, se llevará a cabo en la sede del Centro de Instrucción elegido por el contratista o en forma virtual, conforme se indica en el numeral 6.1 de los términos de referencia.</p> <p>7.3. PLAZO DEL SERVICIO.</p> <p>PLAZO DE EJECUCIÓN DE LA PRESTACIÓN PRINCIPAL.</p> <p>El plazo de ejecución de la prestación principal del servicio es de mil noventa y cinco (1095) días calendario, contados a partir del día siguiente de la suscripción del ACTA DE INICIO DEL SERVICIO y al finalizar el Contrato vigente.</p> <p><u>Prevía al inicio del plazo de ejecución</u></p> <ul style="list-style-type: none">• El plazo de entrega del Plan de Trabajo es de hasta cinco (05) días calendario siguientes de la suscripción del contrato.• El plazo máximo de implementación del servicio es de hasta sesenta (60) días calendario siguientes de la suscripción del contrato. <p>PLAZO PRESTACIÓN ACCESORIA: CAPACITACIÓN</p> <p>El plazo de ejecución de la prestación accesoria es de hasta ciento veinte (120) días calendario, contados a partir del día siguiente de la suscripción del ACTA DE INICIO DEL SERVICIO.</p>												
8	ENTREGABLES DEL SERVICIO	<p>Entregables de la prestación principal:</p> <p>De acuerdo a lo definido en el numeral 5.2. Plan de Trabajo. El Contratista debe entregar el "Plan de Trabajo" en medio físico o digital, en Mesa de Partes situada en Jr. Bolivia N° 109-Lima –primer piso, Edificio del Centro Cívico, en el horario de 08:30 am a 5:00 pm. o Mesa de Partes virtual (https://apps.reniec.gob.pe/MesaPartesVirtual/), dirigido a la Unidad de Infraestructura y soporte tecnológico de la Oficina de Tecnología de la información.</p> <table border="1"><thead><tr><th>ENTREGABLE</th><th>DESCRIPCIÓN</th><th>PLAZO DE ENTREGA DEL ENTREGABLE</th></tr></thead><tbody><tr><td>Primer Entregable</td><td>Informe de culminación de la etapa de implementación (INFORME FINAL DE IMPLEMENTACIÓN)</td><td>Dentro de los tres (3) días calendario siguientes de la culminación de la implementación del servicio, conforme se indica en el numeral 7.3 de los términos de referencia.</td></tr><tr><td>Segundo Entregable</td><td>Informe de ejecución de culminación del primer año del servicio (Informe anual de servicio).</td><td>Dentro de los cinco (05) días calendario siguientes de la culminación del primer año de la prestación del servicio.</td></tr><tr><td></td><td></td><td></td></tr></tbody></table>	ENTREGABLE	DESCRIPCIÓN	PLAZO DE ENTREGA DEL ENTREGABLE	Primer Entregable	Informe de culminación de la etapa de implementación (INFORME FINAL DE IMPLEMENTACIÓN)	Dentro de los tres (3) días calendario siguientes de la culminación de la implementación del servicio, conforme se indica en el numeral 7.3 de los términos de referencia.	Segundo Entregable	Informe de ejecución de culminación del primer año del servicio (Informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del primer año de la prestación del servicio.			
ENTREGABLE	DESCRIPCIÓN	PLAZO DE ENTREGA DEL ENTREGABLE												
Primer Entregable	Informe de culminación de la etapa de implementación (INFORME FINAL DE IMPLEMENTACIÓN)	Dentro de los tres (3) días calendario siguientes de la culminación de la implementación del servicio, conforme se indica en el numeral 7.3 de los términos de referencia.												
Segundo Entregable	Informe de ejecución de culminación del primer año del servicio (Informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del primer año de la prestación del servicio.												





		<table border="1"> <tr> <td>Tercer Entregable</td> <td>Informe de ejecución de culminación del segundo año del servicio (informe anual de servicio).</td> <td>Dentro de los cinco (05) días calendario siguientes de la culminación del segundo año de la prestación del servicio.</td> </tr> <tr> <td>Cuarto Entregable</td> <td>Informe de ejecución de culminación del tercer año del servicio (informe anual de servicio).</td> <td>Dentro de los cinco (05) días calendario siguientes de la culminación del tercer año de la prestación del servicio.</td> </tr> </table>	Tercer Entregable	Informe de ejecución de culminación del segundo año del servicio (informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del segundo año de la prestación del servicio.	Cuarto Entregable	Informe de ejecución de culminación del tercer año del servicio (informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del tercer año de la prestación del servicio.
Tercer Entregable	Informe de ejecución de culminación del segundo año del servicio (informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del segundo año de la prestación del servicio.						
Cuarto Entregable	Informe de ejecución de culminación del tercer año del servicio (informe anual de servicio).	Dentro de los cinco (05) días calendario siguientes de la culminación del tercer año de la prestación del servicio.						

Descripción de los entregables (segundo, tercero y cuarto).

El contratista debe presentar un "INFORME ANUAL DE SERVICIO" correspondiente al periodo de facturación anual, en el que debe incluir: los niveles de disponibilidad, el detalle de solicitudes de atención presentadas en el periodo, la cantidad de solicitudes, tiempo total y medio de reparación. El mismo detalle de información debe presentarse por cada año del servicio brindado, consolidando toda la información en un solo informe, incluyendo siempre las "conclusiones" y las "recomendaciones" del caso.

Entregables de la prestación Accesorio:

El contratista debe entregar los certificados de participación del curso emitido por la marca a cada participante, en un plazo de treinta (30) días calendarios contados a partir del día siguiente de culminado el dictado del curso correspondiente.

9	FORMA DE PAGO	<p>PRESTACIÓN PRINCIPAL:</p> <p>La entidad se obliga a pagar la contraprestación de la prestación principal a el contratista en cuatro (04) armadas, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado, según el siguiente cuadro:</p> <table border="1"> <tr> <th>N°</th> <th>DESCRIPCIÓN</th> <th>PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.</th> </tr> <tr> <td>Primer pago</td> <td>A la conformidad de la prestación del primer entregable.</td> <td>55 %</td> </tr> <tr> <td>Segundo pago</td> <td>A la conformidad de la prestación del segundo entregable.</td> <td>15%</td> </tr> <tr> <td>Tercer pago</td> <td>A la conformidad de la prestación del tercer entregable.</td> <td>15%</td> </tr> <tr> <td>Cuarto pago</td> <td>A la conformidad de la prestación del cuarto entregable.</td> <td>15%</td> </tr> </table> <p>Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:</p> <ul style="list-style-type: none"> - Conformidad por la prestación principal del servicio emitida por la Oficina de Tecnologías de la Información, previo informe técnico de la Unidad de Infraestructura y Soporte Tecnológico. - Comprobante de pago. <p>Prestación accesoria – Capacitación y/o entrenamiento</p> <p>La entidad se obliga a pagar la contraprestación de la prestación accesoria a el Contratista, en pago único (correspondiente al 100% del monto de la prestación accesoria), luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.</p> <p>Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:</p>	N°	DESCRIPCIÓN	PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.	Primer pago	A la conformidad de la prestación del primer entregable.	55 %	Segundo pago	A la conformidad de la prestación del segundo entregable.	15%	Tercer pago	A la conformidad de la prestación del tercer entregable.	15%	Cuarto pago	A la conformidad de la prestación del cuarto entregable.	15%
		N°	DESCRIPCIÓN	PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.													
		Primer pago	A la conformidad de la prestación del primer entregable.	55 %													
		Segundo pago	A la conformidad de la prestación del segundo entregable.	15%													
		Tercer pago	A la conformidad de la prestación del tercer entregable.	15%													
Cuarto pago	A la conformidad de la prestación del cuarto entregable.	15%															



		<ul style="list-style-type: none"> - Conformidad por la prestación accesoria del servicio emitida por la Oficina de Tecnologías de la Información, previo informe técnico de la Unidad de Infraestructura y Soporte Tecnológico. - Comprobante de pago. <p>Dicha documentación se debe presentar en Mesa de Partes de la Entidad sito en Av. Javier Prado Este N° 990 - San Isidro - Lima o mesa de partes virtual al link: https://apps.reniec.gob.pe/MesaPartesVirtual/.</p>
10	CONFORMIDAD	<p>PRESTACIÓN PRINCIPAL</p> <p>La conformidad de la prestación principal del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la Oficina de Tecnologías de la Información, previo informe técnico de la Unidad de Infraestructura y Soporte Tecnológico, en el plazo máximo de siete (7) días de producida la recepción.</p> <p>PRESTACIÓN ACCESORIA –CAPACITACIÓN</p> <p>La conformidad de la prestación accesoria del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la Oficina de Tecnologías de la Información, previo informe de la Unidad de Infraestructura y Soporte Tecnológico, en el plazo máximo de siete (7) días de producida la recepción.</p>
11	PENALIDADES	<p>PENALIDADES</p> <p>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:</p> $\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$ <p>Donde:</p> <p>F = 0.25 para plazos mayores a sesenta (60) días o;</p> <p>F = 0.40 para plazos menores o iguales a sesenta (60) días.</p> <p>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.</p> <p>OTRAS PENALIDADES APLICABLES DE LA PRESTACIÓN PRINCIPAL</p> <p>Conforme establece el artículo 163 del Reglamento de la ley de Contrataciones del Estado, la entidad tiene la potestad de establecer penalidades, las mismas que son</p> <p>PRESTACIÓN PRINCIPAL</p>





N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de Verificación
1	Retraso injustificado en la entrega del informe anual del servicio mayor al plazo establecido en el numeral 8 de los términos de referencia.	10% de una UIT por cada día de retraso y ocurrencia.	La Unidad de Infraestructura y Soporte Tecnológico debe verificar y controlar el cumplimiento del plazo de entrega del informe anual.

PRESTACIÓN ACCESORIA

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de Verificación
2	Demora en la asignación de tickets de las solicitudes o incidentes reportadas por el RENIEC mayor a 15 minutos, según literal B) (SOPORTE TÉCNICO) de los términos de referencia.	10% de una UIT, por cada 5 minutos adicionales de demora en generar los tickets y por ocurrencia.	La Unidad de Infraestructura y Soporte Tecnológico verificará el cumplimiento en el informe anual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el año.
2	Demora en la resolución de las solicitudes y/o incidentes Críticos o Altos >2 horas, según literal B) (SOPORTE TÉCNICO) de los términos de referencia.	1/60 de UIT por cada minuto adicional y por ocurrencia. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido.	La Unidad de Infraestructura y Soporte Tecnológico verificará el cumplimiento en el informe anual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el año.
3	Demora en la resolución de las solicitudes y/o incidentes Medios o Moderados >4 horas, según literal B) (SOPORTE TÉCNICO) de los términos de referencia	1/120 de UIT por cada minuto adicional y por ocurrencia. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido.	La Unidad de Infraestructura y Soporte Tecnológico verificará el cumplimiento en el informe anual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el año.



			D	Demora en la resolución de las solicitudes y/o incidentes Bajos >8 horas, según literal B) (SOPORTE TÉCNICO) de los términos de referencia	1/240 de UIT vigente por cada minuto adicional y por ocurrencia. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido.	La Unidad de Infraestructura y Soporte Tecnológico verificará el cumplimiento en el informe anual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el año.
<i>* La UIT referida debe ser vigente a la fecha de ocurrida la penalidad.</i>						
12	SISTEMA DE CONTRATACIÓN	Suma alzada				
13	RESPONSABILIDAD POR VICIOS OCULTOS	<p>La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.</p> <p>El plazo máximo de responsabilidad del contratista es un (01) año contado a partir de la conformidad otorgada por LA ENTIDAD.</p>				
14	CONFIDENCIALIDAD	<p>El contratista se obliga a mantener la confidencialidad y reserva absoluta en el manejo de información a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros.</p> <p>En tal sentido, el contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido la prestación. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista.</p>				
15	MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL	<p>El Contratista y la Unidad de Infraestructura y Soporte Tecnológico del RENIEC, realizarán el monitoreo continuo al servicio, a fin de asegurar que los servicios serán brindados de conformidad con lo solicitado en los términos de referencia.</p> <p>Todos los costos que demanden la realización del monitoreo serán asumidos por el Contratista.</p> <p>Cualquier incidente identificado deberá ser atendido en cumplimiento a los Acuerdos de niveles de servicio, descritos en el numeral 5-B del TDR.</p>				
16	CLÁUSULA ANTICORRUPCIÓN	<p>EL CONTRATISTA 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 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.</p> <p>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, participacionistas, integrantes de los órganos de</p>				



	<p>administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.</p> <p>Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.</p> <p>Sírvase verificar la Política Antisoborno del Registro Nacional de Identidad y Estado Civil, en la siguiente ruta web: https://www.reniec.gob.pe/portal/html/institucional/politicas_antisoborno_2022.pdf</p> <p>Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.</p>
REQUISITOS DE CALIFICACIÓN	
A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1	CALIFICACIONES DEL PERSONAL CLAVE
A.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>JEFE DEL PROYECTO</p> <ul style="list-style-type: none"> • Titulado en las carreras de Ingeniería electrónica, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniero Informático o Ingeniero Industrial, o Ingeniería Empresarial y de Sistemas. <p>ESPECIALISTA DE SOPORTE TÉCNICO</p> <ul style="list-style-type: none"> • Titulado o Bachiller en las carreras de Ingeniería electrónica, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniero Informático o Ingeniero Industrial, o Ingeniería de Seguridad y Auditoría Informática. <p>ESPECIALISTA EN MONITOREO Y SEGURIDAD GESTIONADA</p> <p>Profesional titulado o Bachiller en las carreras de Ingeniería electrónica, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones y Redes, o Ingeniero Informático o Ingeniero Industrial, o Ingeniería de Seguridad y Auditoría Informática</p> <p><u>Acreditación:</u></p> <p>El Grado o Título será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En caso Grado o Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>



A.1.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>JEFE DEL PROYECTO</p> <p>Experiencia mínima a cinco (05) años como Jefe y/o Supervisor de proyectos, en proyecto de TI o ciberseguridad.</p> <p>ESPECIALISTA DE SOPORTE TÉCNICO</p> <ul style="list-style-type: none"> Experiencia mínima de cinco (05) años en servicio de instalación y/o Configuración y/o Administración y/o Soporte y/o Mantenimiento de: Soluciones de Filtro de Contenido Web. <p>ESPECIALISTA EN MONITOREO Y SEGURIDAD GESTIONADA</p> <ul style="list-style-type: none"> Experiencia mínima de cinco (05) años en servicio de Monitoreo y/o seguridad gestionada, en Soluciones de Filtro de Contenido Web. <p><u>Acreditación:</u></p> <p>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> <div data-bbox="395 891 1353 1384" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <ul style="list-style-type: none"> 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 anteriores a la fecha de la presentación de ofertas. Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases. </div>
B	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1,400,000.00 (Un millón cuatrocientos mil y 00/100 soles), por la contratación de servicios 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 servicios similares a los siguientes:</p> <ul style="list-style-type: none"> Servicio de soporte y/o mantenimiento y/o renovación, de licencias de filtro de contenido web y/o Servicio de soporte y/o mantenimiento y/o renovación, de licencias de solución de seguridad de aplicación móvil y/o Servicio de soporte y/o mantenimiento y/o renovación, de licencia de firewall de aplicación web y/o Servicio de soporte y/o mantenimiento y/o renovación, de licencia de Firewall de siguiente



- generación y/o
- Servicio de soporte y/o mantenimiento y/o renovación, de Firewall de siguiente generación y/o
- Servicio de soporte y/o mantenimiento y/o renovación, de licencias de ciberseguridad.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, 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 pago¹, correspondientes a un máximo de veinte (20) contrataciones.

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.

En el caso de servicios de ejecución periódica o continuada, 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.

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.

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.

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.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios 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 servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante

¹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".



- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *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".*



LUIS ENRIQUE GALLEGOS HUAMANI
Jefe de Unidad de Infraestructura y Soporte Tecnológico
REGISTRO NACIONAL DE IDENTIFICACIÓN
Y ESTADO CIVIL