

		REQUERIMIENTO PARA LA CONTRATACIÓN DE SERVICIOS
1	AREA USUARIA	Unidad de Infraestructura y Soporte Tecnológico de la Oficina de Tecnologías de la Información (UIST)
2	DENOMINACIÓN DE LA CONTRATACIÓN	SERVICIO DE SEGURIDAD PARA CORREO ELECTRONICO
3	FINALIDAD PÚBLICA DE LA CONTRATACIÓN	Se requiere contratar el “Servicio de Seguridad para Correo electrónico”, el servicio requerido es referido a la protección de la infraestructura de correo Institucional ante ataques informáticos con correos SPAM, correos con publicidad no solicitados, correos Phishing, correos maliciosos de Ingeniería Social, mensajes con archivos maliciosos, adjuntos con virus de día cero, amenazas de malware avanzado y fuga de información. El requerimiento del servicio garantizará la confidencialidad, integridad y disponibilidad de las comunicaciones que el RENIEC realiza a través del servicio de Correo Institucional.
4	OBJETIVO GENERAL DE LA CONTRATACIÓN	Consiste en la contratación de una persona natural o jurídica especializada en seguridad informática y/o información y/o seguridad de correos electrónicos, que provea un “Servicio de Seguridad para Correo electrónico”, por el periodo de treinta y seis (36) meses, contados luego de culminar la etapa de implementación del servicio, que permita garantizar y asegurar la continuidad del servicio de correo electrónico de los usuarios finales del RENIEC.
5	ALCANCES Y ACTIVIDADES A DESARROLLAR	<p>5.1. ALCANCE Y DESCRIPCIÓN DEL SERVICIO.¹</p> <p>El servicio ofertado debe proporcionar equipamiento de seguridad tecnológica, siendo responsabilidad del proveedor garantizar la compatibilidad, integración, interoperabilidad y funcionalidad entre los componentes del servicio solicitado y las soluciones de seguridad preexistente en el RENIEC. El contratista implementará la infraestructura tecnológica relacionada al servicio requerido con las capacidades y funcionalidades que le permitan cumplir con los Términos de Referencia y de manera tal que funcionen correctamente durante la vigencia del contrato.</p> <p>El contratista debe ser una empresa con especialización en Seguridad de Correos Electrónicos y como tal debe implementar un servicio de calidad, soportadas por la mejor tecnología disponible en el mercado y con la premisa de conseguir la total integración de las soluciones en caso de implementaciones multimarca. El contratista debe gestionar las soluciones implementadas para la provisión de su servicio y debe estar comprometido a satisfacer la demanda requerida por el servicio, incluyendo proyectos de implementación/migración/integración de sus servicios con otras plataformas, prestando asesoría técnica en materia de tecnología durante el periodo de ejecución del servicio; participando inclusive en los diseños, topologías, en las implementaciones y la gestión de</p>



¹ Ver Respuesta: N° 22 del Pliego de Absolución de Consultas y Observaciones

		<p>dichos proyectos. Esto no incluye el aprovisionamiento de equipamiento adicional.</p> <p>El contratista es responsable de la instalación y/o implementación de todos los equipos que conforman la solución para brindar el servicio requerido. Antes de la instalación de los equipos debe identificar que el tipo de toma de cada equipo sea compatible con los PDU (del tipo C-13) instalados en los gabinetes del RENIEC, identificar la profundidad y el tipo de ranura de los ejes verticales para el rackeo respectivo. Asimismo, el contratista es responsable de proveer e instalar el cableado necesario para la operatividad de cada uno de los equipos que conforman las soluciones ofertadas y su conectividad e integración con cada uno de los componentes del servicio, en caso de cableado de cobre debe ser CAT6A y en caso de fibra óptica multimodo los conectores deben ser LC.</p> <p>La solución de seguridad de correo electrónico que se implementaran para el cumplimiento de la prestación del servicio debe contar con consolas de administración para la gestión respectiva. Esta consola debe ser dedicada, de acuerdo a la solución, en equipamiento provisto por el contratista y deben instalarse en la Sede San Borja del RENIEC. El contratista debe garantizar la performance y buen rendimiento de la consola de gestión, instalada como parte del servicio.</p> <p>El dimensionamiento del equipamiento de la consola será de total responsabilidad del contratista, toda vez que esta debe ofrecer un óptimo rendimiento de operación, así como su diseño y topología. El Contratista debe garantizar durante el periodo de contrato el soporte técnico de hardware/software y garantía de la solución provista. Asimismo, el Contratista debe garantizar el almacenamiento de seis (6) meses de logs, estos logs deben estar disponibles cuando el RENIEC lo requiera.</p> <p>El contratista debe garantizar que el hardware de la solución que se implemente para brindar el servicio solicitado sea nuevo y de primer uso y con fecha de fabricación no mayor a un año. El hardware y software de las soluciones deben tener garantía y soporte de fábrica, por el periodo de vigencia del contrato, ante defectos de fabricación, fallas de los componentes internos, que causen inoperatividad o mal funcionamiento de la solución, para proceder con el reemplazo de hardware o software correspondiente, el cual no debe exceder de los sesenta (60) días calendario contados a partir del día siguiente del diagnóstico correspondiente, sin costo para la Entidad. Además, debe garantizarse durante la vigencia del contrato, que en caso el fabricante publique el anuncio de Fin de Ciclo de Vida de alguno de los equipos implementados, éstos serán reemplazados por su actualización tecnológica correspondiente en coordinación con los especialistas de la Unidad de Infraestructura y Soporte Tecnológico (UIST) y sin costo adicional para el RENIEC. En caso de existir un reemplazo, el mismo deberá realizarse antes del fin de soporte anunciada por el fabricante para los equipos.</p> <p>Durante la vigencia del contrato, el contratista debe realizar dos mantenimientos preventivos durante el periodo de ejecución del contrato, a todas las soluciones implementadas, a fin de asegurar la operatividad de todos los componentes del servicio. El primer mantenimiento se ejecutará al finalizar el primer año del servicio y el siguiente al finalizar el segundo año del servicio.</p>
--	--	--



El Contratista será responsable de mantener actualizada la solución implementada con las últimas versiones estables de sus sistemas operativos y en caso corresponda con las últimas firmas de ataque, firmas de virus y/o malwares, bases de datos de aplicaciones, categorización de URLs y todas las nuevas funcionalidades de protección y análisis que correspondan. El contratista debe asegurar y garantizar al RENIEC el óptimo funcionamiento y rendimiento de la solución implementada, bajo los parámetros establecidos por el fabricante, debiendo realizar los ajustes de capacidades de hardware/software necesarios si se detecta recurrencia en la degradación de rendimiento de dicha solución; si para la actualización o upgrade de los sistemas operativos implique realizar un mejoramiento de las capacidades de la solución (CPU, Memoria, Disco) o realizar un upgrade de la solución, estas deben ser asumidas por el Contratista sin costo adicional para el RENIEC. Además, cuando se identifiquen vulnerabilidades en los sistemas o infraestructura que soporta la solución implementada en este servicio, el Contratista debe ejecutar la remediación correspondiente en coordinación con los especialistas de la Unidad de Infraestructura y Soporte Tecnológico (UIST).

A continuación, se describen los componentes del “Servicio de Seguridad para Correo electrónico”:

- Servicio de protección ante ataques informáticos con correos SPAM, correos con publicidad no solicitados, correos Phishing, correos maliciosos de Ingeniería Social, mensajes con archivos maliciosos, adjuntos con virus de día cero, amenazas de malware avanzado y fuga de información.
- Servicio de Soporte, mantenimiento, garantía y suscripciones.
- Servicio de Capacitación.



Acuerdo de niveles de servicio (ANS).

ANS	Descripción	Cálculo de la Medición	Valor Base %	Horario Acordado	Periodicidad
Disponibilidad de la consola del servicio de protección del Antispam.	El objetivo de este ANS es medir la disponibilidad de la consola de gestión de la solución de protección del Antispam.	Disponibilidad = $(1 - \text{TIPM/TTS M}) \times 100$	≥ 99.9	24x7	Anual
Disponibilidad del servicio del AntiSpam (por cada sede).	El objetivo de este ANS es medir la disponibilidad de la solución del Antispam en la nube, por cada sede.	Disponibilidad = $(1 - \text{TIPM/TTS M}) \times 100$	≥ 99.9	24x7	Anual

Donde **TIPM: Tiempo de interrupción en el año en minutos.**
TTSM: Tiempo total de servicio en el año en minutos.

		<p>Si la disponibilidad de la consola del servicio de protección del antispam es menor al 97%, hasta en dos (02) oportunidades durante dos (2) meses consecutivos, el Contratista debe reemplazar la solución, por otra solución de iguales o superiores características, sin costo para la Entidad. Para la provisión de la solución de reemplazo el Contratista tiene un plazo de sesenta (60) días calendario, contados a partir del día siguiente de recibida la notificación por parte del RENIEC. El Contratista debe garantizar la continuidad del servicio de protección del Antispam.</p> <p>Si la disponibilidad de la solución de protección del AntiSpam perimetral (por cada sede) es menor al 97% en base anual, en hasta dos (2) oportunidades durante dos (02) meses consecutivos, el Contratista debe reemplazar la solución, por otra solución de iguales o superiores características, sin costo para la Entidad y sin que esto exima las penalidades correspondientes. Para el reemplazo de la solución, el Contratista tiene un plazo de sesenta (60) días, contados a partir del día siguiente de recibida la notificación por parte del RENIEC.</p> <p>5.2. CONSIDERACIONES GENERALES DEL SERVICIO²</p> <p>El Contratista debe proveer el servicio de una solución para la protección de los correos electrónicos, que debe incluir la implementación y puesta en producción del servicio.</p> <p>El Contratista debe implementar una consola de gestión que permita la visibilidad, monitoreo y generación de reportes, ya sea on-premise o en la nube. Debe garantizar el almacenamiento de logs por el lapso de seis (06) meses o en su defecto garantizar al menos un (1) mes de logs para analítica de la solución y cinco (5) meses de logs en servidor syslog adicional pero dentro del mismo servidor físico. Esta consola de gestión deberá contar con un entorno web para realizar las tareas de configuración de la solución propuesto en sitio y debe soportar diferentes niveles de autorización para los usuarios administradores de la misma; además debe ser capaz de personalizar el “dashboard” por usuario de acuerdo a políticas definidas, ello significa que debe ser capaz de limitar el alcance de las configuraciones que puedan realizar distintos usuarios de acuerdo a sus roles. Para soluciones On-Premise se debe visualizar el estado de la solución AntiSpam, consumo de CPU, memoria, conexiones, ataques, entre otros. La consola de gestión debe incluir todo el licenciamiento necesario para una completa y eficiente gestión del servicio.</p> <p>El contratista debe asegurar y garantizar el soporte técnico del fabricante de todo equipamiento informático incluido en la implementación de las soluciones del servicio, en modo 24x7x365. El postor ganador de la buena pro debe presentar la documentación del fabricante que acredite el cumplimiento de este requerimiento, el cual será entregado a la firma del contrato y cuya vigencia debe ser a partir del día siguiente a la suscripción del acta de conformidad del servicio hasta su culminación.³</p>
--	--	--



² Ver Respuesta: N° 23 del Pliego de Absolución de Consultas y Observaciones

³ Ver Respuesta: N° 16, 17 del Pliego de Absolución de Consultas y Observaciones

El postor ganador de la buena pro debe acreditar que el personal clave como Jefe de proyecto debe contar la certificación de ciberseguridad ISO 27032 o Lead Cybersecurity Professional Certificate – LCPSPC, el cual será entregado como requisito para suscripción de contrato, se acreditará con copia simple de constancias, certificados o diploma⁴.

El postor ganador de la buena pro debe acreditar que el profesional para la Implementación debe contar con certificado oficial vigente del fabricante en la solución ofertada,⁵ el cual será entregado como requisito para suscripción de contrato, se acreditará con copia simple de constancias, certificados o diploma.

5.3. CONSIDERACIONES ESPECÍFICAS DEL SERVICIO.

El proveedor debe garantizar la disponibilidad del servicio; asimismo, debe implementar la última versión estable y activar todas las características, módulos, funcionalidades y licencias (suscripciones) de la solución de acuerdo a los requerimientos especificados en el presente término de referencia, los cuales deben ser configurados de acuerdo a las políticas del servicio de correo de RENIEC.

La solución debe proveer funcionalidades y características de protección para 2600 casillas de correo electrónico, tales como se especifican en el ANEXO N° 01 de características Técnicas.

Para lo cual, a la presentación de ofertas, el postor debe entregar la siguiente información técnica:

- ✓ La acreditación del cumplimiento de las características técnicas, adjuntando la documentación oficial del fabricante en idioma inglés o español, ya sean Hojas de Datos (Datasheets), Brochures, Guía técnica de usuario (link y/o manuales de usuario) indicando el número de página, párrafo y texto que valide el cumplimiento. Asimismo, se aceptará en el caso de no existir alguna documentación según lo antes solicitado, una carta de fabricante confirmando el cumplimiento de dicha característica. (ANEXO N° 01 de Características Técnicas).⁶

5.4. GESTIÓN DE SOPORTE Y GARANTÍA DEL SERVICIO.

El contratista debe brindar el servicio de soporte y garantía de buen funcionamiento del servicio implementado, lo que permitirá al RENIEC hacer uso de las últimas versiones publicadas por el fabricante, ediciones (releases), actualizaciones disponibles en el mercado, análisis de eventos, consultas técnicas y resolución de incidencias que se presenten con relación a la funcionalidad u operatividad de la solución implementada.

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



⁴ Ver Respuesta: N° 18 del Pliego de Absolución de Consultas y Observaciones

⁵ Ver Respuesta: N° 26 del Pliego de Absolución de Consultas y Observaciones

⁶ Ver Respuesta: N° 9, 55 del Pliego de Absolución de Consultas y Observaciones

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 tickets⁷ 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 deresolución
Crítico o alto	In site o Asistencia remota	2 horas
Medio o Moderado	In site o Asistencia remota	4 horas
Bajo	Asistencia Remota	8 horas

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

El tiempo máximo de resolución será contabilizado a partir de la generación de ticket correspondiente. El contratista brindará al RENIEC los enlaces o contactos de comunicación para hacer efectivos los reportes de incidente o eventos.



5.5. ACTIVIDADES.

1. Reunión de KickOff, a los dos (2) días calendario de firmado el contrato. El contratista presentará a su personal responsable por cada uno de los proyectos a implementar.
2. Visitas técnicas del contratista a las instalaciones del RENIEC, Centro de Datos "Housing" y sede San Borja. El cronograma de visitas será definido en la reunión de KickOff.
3. Reuniones con el Contratista para tratar los temas de diseño de las topologías de las soluciones a implementar para la provisión del servicio. El cronograma de reuniones será definido en la reunión de KickOff.
4. Entrega del Plan de Trabajo del Servicio, dentro de los diez (10) días calendario siguientes a la suscripción del contrato.
5. Aprobación del Plan de Trabajo del Servicio por parte de la Unidad de Infraestructura y Soporte Tecnológico, dentro de los tres (3) días de recibido el plan de trabajo.
6. Reuniones con el Contratista para tratar temas de la implementación de la solución ofertada para brindar el servicio.
7. Protocolo de pruebas para el servicio implementado de los componentes del servicio.
8. Conformidad de la Implementación del servicio.
9. Inicio del servicio.

⁷ Ver Respuesta: N° 52 del Pliego de Absolución de Consultas y Observaciones

		<p>5.6. PLAN DE TRABAJO DEL SERVICIO</p> <p>Planteamiento del Proyecto Dentro de los diez (10) 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, instalación, configuración y puesta en operación de cada uno de los componentes de la prestación del servicio; además, debe incluir como mínimo los siguientes rubros:</p> <ul style="list-style-type: none"> a. Planeamiento de Red y Seguridad: Descripción de la arquitectura/topología, descripción de actividades, análisis y diseño, detallando las soluciones que implementará el Contratista. b. Aprovisionamiento de Equipos: Descripción del listado general de equipos que se instalarán para el servicio. c. Trabajos de Montaje e Instalación: Descripción del montaje y configuración de los equipos. d. Pruebas de Aceptación y puesta en Servicio: Descripción del Protocolo de Pruebas para la aceptación y monitoreo de los Niveles de Servicio, pruebas de parámetros de Niveles de Servicio. El protocolo de pruebas propuesto será validado por el RENIEC conjuntamente con el Contratista. e. Cronograma: Diagrama de Gantt y Desarrollo de PERT. El diagrama Gantt explicará en días el plan de trabajo, indicando las actividades/tareas y el desarrollo PERT permitirá conocer la ruta crítica correspondiente. <p>5.7. INICIO DEL SERVICIO</p> <p>El inicio del servicio se contará a partir del día siguiente de culminada la etapa de implementación, con la suscripción del acta de conformidad por la implementación y culminado el contrato vigente.</p> <p>Para dar inicio al servicio, se debe emitir previamente el Acta de Conformidad por la Implementación y migración total del servicio, que será suscrita por el Contratista y la Unidad de Infraestructura y Soporte Tecnológico del RENIEC. Para la emisión de la conformidad, el Contratista debe cumplir con todo lo requerido en los presentes términos de referencia, cuyo criterio de validación se basará en el informe final de la Implementación emitido por el Contratista.</p> <p>En calidad informativo, el contratista dentro de los cinco (5) días calendario posteriores a la implementación total del servicio, el Contratista debe entregar por Mesa de Partes Virtual un Informe Final de la Implementación en formato digital (PDF), donde se detallen el servicio implementado, que contenga por lo menos lo siguiente:</p> <ul style="list-style-type: none"> a. Descripción de la arquitectura implementada y diagrama de la Topología de la red. b. Equipos instalados y/o servicios implementados. c. Configuración del equipamiento instalado. d. Registros de protocolos de pruebas e. 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. f. Procedimiento e información de contacto para solicitudes al área comercial, el cual debe incluir como mínimo: Teléfonos y correo electrónico.
--	--	--



		<p>5.8. RECURSOS A SER PROVISTOS POR EL CONTRATISTA</p> <p>Todos los equipos, materiales y accesorios necesarios, serán provistos por el Contratista. El Contratista debe proporcionar todo el equipamiento que sea necesario para el cumplimiento del servicio (a excepción de lo declarado explícitamente como recurso a ser provisto por el RENIEC, en el numeral 5.9 del presente termino de referencia).</p> <p>Será de total y exclusiva responsabilidad del Contratista contemplar todas las actividades, dispositivos, licencias, componentes y accesorios para la correcta instalación de la solución para brindar el servicio requerido en los plazos mencionados.</p> <p>El Contratista será responsable de las siguientes actividades requeridas para el suministro del servicio:</p> <ul style="list-style-type: none"> ✓ 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 a suministrar. <p>5.9. RECURSOS A SER PROVISTOS POR LA ENTIDAD</p> <ul style="list-style-type: none"> ✓ El RENIEC brindará todas las facilidades de acceso a sus oficinas al personal del Contratista del servicio y realizará las gestiones correspondientes en el local del Housing. Es responsabilidad del Contratista la gestión de permisos, autorizaciones y licencias para los trabajos que tengan que realizar en espacios que no son propiedad del RENIEC o que estén fuera del local Housing y de existir gastos relacionados al mismo, estos deben ser asumidos por el Contratista. ✓ También se brindará el espacio físico para la implementación en la Sede San Borja.
6	PRESTACIÓN ACCESORIA	<p>CAPACITACIÓN:</p> <p>El contratista debe brindar curso de capacitación en idioma español en la administración de la solución implementada (Antispam), para el personal de la Unidad de Infraestructura y Soporte Tecnológico.</p> <p>La capacitación en la administración de la solución implementada debe cumplir con los siguientes requerimientos a fin de asegurar su idoneidad técnica para el desarrollo de la solución requerido:</p> <ul style="list-style-type: none"> ○ Dictado por instructor certificado por la marca de la solución instalada. ○ 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. ○ 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.



		<ul style="list-style-type: none"> ○ 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, en un plazo de treinta (30) días calendarios contados a partir del día siguiente de culminado el dictado del curso correspondiente. ○ El plan de capacitación con mención de fechas tentativas será entregado para la suscripción del contrato 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. Se aceptará una declaración jurada del postor ganador de la buena pro, en donde se indique que los instructores de los cursos cumplen con las certificaciones necesarias que lo califican para tal fin. ○ 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 DE LA PRESTACIÓN PRINCIPAL.</p> <p>La entrega del servicio se debe realizar en la locación 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.</p> <p>7.3. PLAZO DE LA PRESTACIÓN PRINCIPAL.</p> <p><u>Anterior al inicio del servicio (implementación).</u></p> <ul style="list-style-type: none"> • El plazo de entrega del Plan de Trabajo es de hasta diez (10) días calendario siguientes de la suscripción del contrato. • El plazo de implementación de la solución será de hasta sesenta (60) días calendario, contados a partir del día siguiente de suscrito el contrato.⁸ <p>7.4. PLAZO DE EJECUCIÓN DEL SERVICIO.</p> <p>El plazo de ejecución de la prestación principal del servicio es por treinta y seis (36) meses, contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación y al finalizar el Contrato vigente.</p> <p>7.5. 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 Conformidad por la implementación.</p>

⁸ Ver Respuesta: N° 21 del Pliego de Absolución de Consultas y Observaciones



8	ENTREGABLES DEL SERVICIO	<p>Entregables de la prestación principal:</p> <p>De acuerdo a lo definido en el numeral 5.6. 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 5.6 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>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> </tbody> </table> <p>Descripción de los entregables 2, 3 y 4 posterior al inicio del servicio.</p> <p>El contratista debe presentar un “INFORME ANUAL DE SERVICIO” correspondiente al período de facturación anual, en el que debe incluir: los niveles de disponibilidad, el detalle de solicitudes de atención presentadas en el período, 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.</p> <p>Entregables de la prestación Accesoría:</p> <p>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.</p>	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 5.6 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.	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.
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 5.6 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.															
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.															
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"> <thead> <tr> <th>N°</th><th>DESCRIPCIÓN</th><th>PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.</th></tr> </thead> <tbody> </tbody> </table>	N°	DESCRIPCIÓN	PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.												
N°	DESCRIPCIÓN	PORCENTAJE DEL MONTO DE LA PRESTACIÓN PRINCIPAL.															



		<table border="1"> <tr> <td>Primer pago</td><td>A la conformidad de la prestación del primer entregable.</td><td>70 %</td></tr> <tr> <td>Segundo pago</td><td>A la conformidad de la prestación del segundo entregable.</td><td>10%</td></tr> <tr> <td>Tercer pago</td><td>A la conformidad de la prestación del tercer entregable.</td><td>10%</td></tr> <tr> <td>Cuarto pago</td><td>A la conformidad de la prestación del cuarto entregable.</td><td>10%</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</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> <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. 	Primer pago	A la conformidad de la prestación del primer entregable.	70 %	Segundo pago	A la conformidad de la prestación del segundo entregable.	10%	Tercer pago	A la conformidad de la prestación del tercer entregable.	10%	Cuarto pago	A la conformidad de la prestación del cuarto entregable.	10%
Primer pago	A la conformidad de la prestación del primer entregable.	70 %												
Segundo pago	A la conformidad de la prestación del segundo entregable.	10%												
Tercer pago	A la conformidad de la prestación del tercer entregable.	10%												
Cuarto pago	A la conformidad de la prestación del cuarto entregable.	10%												
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, quien verificará el cumplimiento de los entregables establecidos en el numeral 8. ENTREGABLES DEL SERVICIO de los términos de referencia, 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, quien verificará el cumplimiento de la capacitación establecido en el numeral 6. PRESTACIÓN ACCESORIA – CAPACITACIÓN de los términos de referencia, 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> <p style="text-align: center;">Penalidad Diaria = 0.10 x monto vigente</p>												



F x 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.

OTRAS PENALIDADES APLICABLES DE LA PRESTACIÓN PRINCIPAL

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 calculadas de forma independiente dentro de los parámetros establecidos.

PENALIDAD POR EL INCUMPLIMIENTO DE LOS ACUERDOS DE NIVELES DE SERVICIO (ANS).

Item	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Disponibilidad de la consola del servicio de protección del Antispam < 99.9% ⁹	1 UIT, si la disponibilidad es >= a 99.5 pero < a 99.9%. 2 UIT, si la disponibilidad es >= a 99 pero < a 99.5%. 3 UIT, si la disponibilidad es >= a 97 pero < a 99%. 4 UIT, si la disponibilidad es < a 97%.	La Unidad de Infraestructura y Soporte Tecnológico debe contrastar el cumplimiento de los ANS acumulados durante el año de ejecución, en el entregable anual del Proveedor.
B	Disponibilidad del servicio AntiSpam de la Sede San Borja < 99.9%	2 UIT, si la disponibilidad es >= a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es >= a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es >= a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Unidad de Infraestructura y Soporte Tecnológico debe contrastar el cumplimiento de los ANS acumulados durante el año de ejecución, en el entregable anual del Proveedor.



⁹ Ver Respuesta: N° 53 del Pliego de Absolución de Consultas y Observaciones

C	Disponibilidad del servicio de protección contra ataques a las aplicaciones web del Centro de Datos "Housing" < 99.9%	2 UIT, si la disponibilidad es >= a 99.5 pero < a 99.9%.	La Unidad de Infraestructura y Soporte Tecnológico debe contrastar el cumplimiento de los ANS acumulados durante el año de ejecución, en el entregable anual del Proveedor.
		4 UIT, si la disponibilidad es >= a 99 pero < a 99.5%.	
		6 UIT, si la disponibilidad es >= a 97 pero < a 99%.	
		8 UIT, si la disponibilidad es < a 97%.	

PENALIDAD POR EL INCUMPLIMIENTO DE LOS OBJETIVOS DEL SERVICIO.¹⁰

Item	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Ataques consolidados de malware o Spam que no fue detectado por la solución implementada.	1 UIT, por cada caso identificado.	La Unidad de Infraestructura y Soporte Tecnológico debe contrastar el cumplimiento de los objetivos del servicio, en el entregable anual del contratista.

PENALIDAD POR EL INCUMPLIMIENTO DE LOS PLAZOS DE EJECUCIÓN DEL SERVICIO DEL CAMBIO/REEMPLAZO DE SOLUCIONES, SEGÚN SEA EL CASO, POSTERIOR AL INICIO DE SERVICIO.

Item	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Plazo para reemplazo de una consola de gestión > a 60 días.	10% de una UIT, por cada día de atraso y ocurrencia.	La Unidad de Infraestructura y Soporte Tecnológico debe verificar y controlar los días de atraso del plazo para el reemplazo de la consola correspondiente.
B	Reemplazo de hardware o Software por fallas de fabricación, mayor a 60 días calendario.	10% de una UIT, por cada día de atraso y ocurrencia.	La Unidad de Infraestructura y Soporte Tecnológico debe verificar y controlar los días de atraso del plazo para el reemplazo de la consola correspondiente.

PENALIDAD POR EL INCUMPLIMIENTO EN LA ENTREGA DE LOS INFORMES ANUALES.



¹⁰ Ver Respuesta: N° 5 del Pliego de Absolución de Consultas y Observaciones

Item	Incumplimiento	Penalidad	Procedimiento de Verificación
A	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.

PENALIDAD DEL INCUMPLIMIENTO EN LOS TIEMPOS DE ATENCIÓN DE INCIDENTES O REQUERIMIENTOS

Item	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Demora en la asignación de tickets de las solicitudes o incidentes reportadas por el RENIEC. >a 15minutos.	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.
B	Demora en la resolución de las solicitudes y/o incidentes Críticos o Altos >2 horas	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.
C	Demora en la resolución de las solicitudes y/o incidentes Medios o Moderados >4 horas	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.



		<table><tr><td>D</td><td>Demora en la resolución de las solicitudes incidentes Bajos horas</td><td>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.</td><td>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.</td></tr></table>	D	Demora en la resolución de las solicitudes incidentes Bajos horas	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.
D	Demora en la resolución de las solicitudes incidentes Bajos horas	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	La presente contratación se rige por el sistema de 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>Toda la información del RENIEC, a que tenga acceso el contratista, así como su personal, es estrictamente confidencial. El contratista y su personal deben comprometerse a mantener las reservas del caso y no trasmitirla a ninguna persona (natural o jurídica), sin la autorización expresa y por escrito del RENIEC.</p> <p>Sobre la inobservancia del párrafo anterior, esta se entenderá como un incumplimiento que no puede ser revertido, por lo que se procederá a la resolución del contrato, bastando para ello una comunicación notarial.</p>				



15	<p>CLÁUSULA ANTICORRUPCIÓN</p> <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 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>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	FORMACION ACADEMICA
	<p>JEFE DE PROYECTO (01)</p> <p><u>Requisitos</u></p> <p>Ingeniero titulado en: Sistemas o electrónica o telecomunicaciones o informática o computación o empresarial y sistemas; del personal clave requerido como jefe de proyectos para ejecutar la función de liderar la implementación del servicio requerido.¹¹</p> <p><u>Acreditación</u></p> <p>El grado o título profesional será verificado 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 el grado o título no se encuentre inscrito en el referido registro, el postor debe presentar la copia simple del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>PROFESIONAL PARA LA IMPLEMENTACIÓN (01)¹²</p> <p><u>Requisitos</u></p>



¹¹ Ver Respuesta: N° 25 del Pliego de Absolución de Consultas y Observaciones

¹² Ver Respuesta: N° 6 del Pliego de Absolución de Consultas y Observaciones

	<p>Ingeniero titulado en: Sistemas o electrónica o telecomunicaciones o informática o computación; del personal clave requerido como profesional para apoyo en la implementación, para ejecutar la función de implementación, configuración y puesta en producción del servicio requerido.</p> <p><u>Acreditación</u></p> <p>El grado o título profesional será verificado 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 el grado o título no se encuentre inscrito en el referido registro, el postor debe presentar la copia simple del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	<p>CAPACITACIÓN¹³</p> <p>Requisitos:</p> <p>JEFE DE PROYECTO (01)</p> <p>Jefe de Proyecto debe contar con capacitación en:</p> <ul style="list-style-type: none"> - Curso de Gestión de la Ciberseguridad desde un enfoque corporativo, bajo los lineamientos de la ISO27032 con al menos 20 horas académicas. - Curso de Gestión de Proyectos bajo el enfoque de la ISO 21502 o Curso PMP con al menos 20 horas académicas. - Implementador Líder ISO27001 con al menos 80 horas académicas. <p>Acreditación: Se acreditará con copia simple de constancias, certificados, u otros documentos, según corresponda.</p>
B.3.3	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p>Requisitos:</p> <p>JEFE DE PROYECTO (01)</p> <p>Experiencia mínima de cuatro (04) años liderando proyectos que comprendan alguna de las siguientes actividades:</p> <ul style="list-style-type: none"> • Instalación y/o implementación de soluciones de seguridad informática y/o, • Instalación y/o supervisión de soluciones de seguridad informática y/o, • Instalación y/o gestión de soluciones de seguridad informática y/o, • Gestión y/o supervisión de data center. <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>PROFESIONAL PARA LA IMPLEMENTACIÓN (01)</p>



¹³ Ver Respuesta: N° 54 del Pliego de Absolución de Consultas y Observaciones

Experiencia mínima de cuatro (04) años diseñando e implementando soluciones de seguridad informática y/o Seguridad de correo electrónico.

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.

C

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD¹⁴

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 1,500,000.00 (un millón quinientos 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.

Se consideran servicios similares a los siguientes:

- Servicio y/o Venta de software, equipamiento o soluciones de Seguridad Informática o Ciber Seguridad que pueden incluir servicios de implementación y/o instalación y/o configuración y/o soporte técnico y/o mantenimiento y/o actualización y/o servicios conexos (asesoría técnica y/o capacitación).
- Servicio de seguridad gestionada.
- Servicio de soporte a los equipos de seguridad perimetral.
- Servicio de soporte a los equipos de prevención y detección de software malicioso.
- Servicio de soporte en seguridad.
- Servicio de implementación de soluciones de seguridad.
- Servicio y/o Venta e Instalación de equipos de seguridad informática: AntiSpam
- Servicio y/o Venta e Instalación de equipos de seguridad informática: Protección de correos electrónicos.

Acreditación:

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 pago¹⁵, 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 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.

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



¹⁴ Ver Respuesta: N° 27 del Pliego de Absolución de Consultas y Observaciones

	<p>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 una persona absorbida 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>		
	<table><tr><td>Importante</td></tr><tr><td><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></td></tr></table>	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>
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>			



ANEXO N° 01 de Características Técnicas

"Servicio de un Sistema Antispam para Asegurar los Correos Electrónicos del RENIEC"					
It	Componentes del Servicio	Funcionalidad	Cumplimiento ¹⁶	Folio	Párrafo que sustente la funcionalidad ¹⁷
	Requerimientos de equipamiento	Si la solución es On Premise esta debe ser capaz de implementarse en appliance con capacidad de ser soportada también en entorno virtual (ESX) como combinación de ambas o completamente como opción en la nube (SaaS) provistas por el mismo fabricante.			
		Si la Solución es On Premise , el appliance debe contar con arreglos RAID y capacidad mínima de 250GB en disco duro.			
		Si la Solución es On Premise debe contar con tarjetas de red 10/100/1000 con capacidad de bonding para alta disponibilidad en caso sea requerida por la solución.			

¹⁶ Ver Respuesta: N° 20 del Pliego de Absolución de Consultas y Observaciones

¹⁷ Ver Respuesta: N° 19, 56, 57 del Pliego de Absolución de Consultas y Observaciones

		Si la Solución es On Premise debe contar con al menos 16 GB de RAM con posibilidad de expansión. Soporte al hardware disponible en la región por el fabricante del mismo en caso sea requerida por la solución			
		Sistema operativo robustecido e integrado con la solución. MTA propietario			
		Si la Solución es On Premise : La Administración es vía HTTPS y SSH. Si la Solución es en Nube: La Administración es vía HTTPS y de manera opcional por SSH. ¹⁸			
		Si la Solución es On Premise debe tener la capacidad de configurar en modo de alta disponibilidad. Capacidad de separar funcionalidades por componente del cluster de acuerdo a las necesidades.			
		Si la solución es SaaS se debe contar con al menos certificación SAS70 o superiores para los sites de procesamiento.			
		Esquema de alta disponibilidad para sitios SaaS con redundancia geográfica.			
		La solución debe ser la misma en cualquier tipo de implementación. ¹⁹			
		Si la Solución es On Premise , la configuración en appliance debe permitir ejecutar todos los engines de AS y AV y Sandboxing sin precisar de plataformas adicionales o de terceros.			
		La Solución debe ser capaz de integrarse con cualquier plataforma de Mensajería, ejemplo Microsoft Exchange, google apps, lotus notes, O365 en al menos sus 3 últimas versiones. ²⁰			
Requerimientos de protección Anti-virus		Deberá realizar el análisis de antivirus tanto conocidos como de día cero, permitiendo la actualización automática del motor y la creación de reglas de análisis de acuerdo a los requerimientos de la organización			
		Deberá contar con un engine de hora cero para poder identificar y contener ataques nuevos para los que no haya firmas.			
		El Anti-virus deberá contar con actualizaciones periódicas que se deben descargar del sitio de la solución de correo y no de la empresa Anti-virus, el deployment de las mismas deberá ser validado para asegurarse de que no existan efectos secundarios que afecten el tráfico.			
		Los correos con amenazas deberán ser contenidos en áreas divididas por engine de detección y su Gestión por área debe ser independiente			
		Cualquiera de los engines propuestos debe tener la capacidad de detectar y bloquear: virus conocidos a través de firmas, mensajes corruptos sospechosos, mensajes que contengan Riskware/Spyware, Phishing así como permitir bloquear mensajes con archivos cifrados.			
		Capacidad de configurar los engines basado en políticas de: rutas, grupos de usuarios, grupos de dominios, usuarios y direcciones IP. Esto en cualquier dirección de tráfico.			



¹⁸ Ver Respuesta: N° 7, 28, 30 del Pliego de Absolución de Consultas y Observaciones

¹⁹ Ver Respuesta: N° 29 del Pliego de Absolución de Consultas y Observaciones

²⁰ Ver Respuesta: N° 8, 31, 51 del Pliego de Absolución de Consultas y Observaciones

Requerimientos de Anti spam	Para el engine de protección de ataques de hora cero, se debe permitir que un correo sospechoso sea reprocesado después de recibir actualizaciones a las firmas.			
	Cualquiera de los engines debe ser capaz de identificar archivos o códigos maliciosos en el contenido del correo, identificando siempre la extensión original.			
	La solución debe contar con un sistema de reputación propietario no dependiente del resto de los engines de detección, que opere tanto para los correos como para los correos de entrada.			
	La detección de tráfico malicioso debe poder realizarse tanto para tráfico de entrada como de salida, permitiendo el control e identificación de ataques internos.			
	La solución deberá permitir identificar amenazas mediante puntajes de los distintos engines a través de la correlación de los mismos, la información debe ser mostrada al administrador a través de la consola para que pueda tomar acciones o tener el detalle de las acciones aplicadas. ²¹			
	La solución debe permitir la modificación de los umbrales de detección de acuerdo a las necesidades de la empresa, así como la creación de perfiles para distintas rutas, dominios, usuarios o direcciones IP, tanto para correo entrante como para correo saliente. ²²			
	Los engines de detección deben actualizarse regularmente y las actualizaciones deben ser descargadas del site del fabricante una vez probados para evitar cualquier impacto al tráfico.			
	Los engines de detección deben ser configurables de forma independiente para poder tropicalizarlos a los requerimientos de la empresa, tales como distintas reglas para ip's, dominios, grupos de usuarios, usuarios, etc.			
	La Solución debe poderse configurar para bloquear correos de marketing o similares (Bulk Mail).			
	La solución debe ser capaz de contener el correo de phishing estándar.			
	La Solución debe poder configurar listas blancas y negras para los engines de Anti-Spam, tanto a nivel General como individual de así precisarse.			
	Se debe contar con la granularidad que permita que el administrador genere reglas para mensajes específicos tanto permisivos como restrictivos que hagan override a las reglas estándar definidas por la solución. Ya para ip's, dominios, usuarios, etc.			
	Las políticas de control de SPAM deben ser modificables, ejemplo que permita tener distintas reglas para el tráfico de entrada del tráfico de salida.			
	Las reglas o políticas de bloqueo deben poder configurarse desde una sola ventana o interfaz.			
	Debe contar con soporte para análisis de DKIM para el tráfico entrante			
	Debe contar con soporte para análisis de SPF para el tráfico entrante			
	Debe soportar con soporte para análisis de DMARC para tráfico entrante			



²¹ Ver Respuesta: N° 32 del Pliego de Absolución de Consultas y Observaciones

²² Ver Respuesta: N° 33 del Pliego de Absolución de Consultas y Observaciones

	Debe contar con una herramienta para bouncing que permita llaves fijas y dinámicas estas últimas generadas sin necesidad de intervención. ²³			
	Debe poseer la funcionalidad de control de SMTP, volúmenes, recurrencia, hosts, etc, para controlar ataques tanto internos como externos.			
	Poseer integración con directorio activo o bases de datos para verificación de usuarios. No necesaria para la operación de la plataforma.			
	La herramienta debe contar con reportes a usuario final que permitan tomar acciones como liberar o notificar spam, vía correo electrónico o bien a través de un portal de usuario. Que pueda configurarse desde, para un usuario como para un grupo o bien a toda la empresa			
	Debe contar con la capacidad de utilizar exportar reportes en formato csv y/o pdf y/o html			
	Las opciones de las notificaciones a usuario final deben poder ser configurables por el administrador para restringir o habilitar funcionalidades ²⁴			
	Debe contar con áreas de cuarentena específicas por engine.			
	El módulo debe tener la capacidad de configurarse para distintas rutas, direcciones y dominios.			
	Debe permitir la utilización de diccionarios específicos que permitan la búsqueda de palabras, frases e incluso expresiones regulares, mismas que serán revisadas en cualquier correo ya en el header, body, attachment y footer.			
	La solución debe Soportar configuraciones para limitar los archivos adjuntos que se envíen o reciben.			
	Debe tener la capacidad de que el usuario pueda auto gestionar su propia cuarentena de mensajes.			
	Debe manejar múltiples carpetas o tipos de cuarentena donde puedan recibir acciones predeterminadas como retención y/o liberación manual del mensaje en cuarentena			
	Debe tener la capacidad de controlar el tamaño de cuarentena.			
	Deberá tener la capacidad de controlar el tiempo de los mensajes en cuarentena			
	La efectividad de la solución para proteger de correo spam debe ser al menos 99%			
	Deberá tener la capacidad de marcar los correos en el subject como SPAM. ²⁵			
	La solución debe poder permitir imprimir un mensaje personalizado que certifique el análisis del correo en calidad de aviso legal.			



²³ Ver Respuesta: N° 40 del Pliego de Absolución de Consultas y Observaciones

²⁴ Ver Respuesta: N° 41 del Pliego de Absolución de Consultas y Observaciones

²⁵ Ver Respuesta: N° 34 del Pliego de Absolución de Consultas y Observaciones

	La solución debe poder ser configurado para aceptar correo electrónico de un número limitado de dominios.			
Requerimientos de la consola	Acceso a la consola vía HTTPS y SSH			
	Gestión de administradores por niveles y perfiles de acceso			
	Passwords administrativos configurables para cumplir los requerimientos de la empresa.			
	Gestión de puertos para control de acceso a los administradores y usuarios. ²⁶			
	Debe contar con la opción de enviar y recibir correo cifrado de dominio a dominio a través de TLS/SSL y permitir agregar los certificados públicos de dominios confiables.			
	Debe contar con un reporte de utilización del equipo por engine.			
	Debe contar con un reporte de que muestre el estado de cada equipo que conforma la solución ²⁷			
	Debe contar con un sistema de alertas que permita monitorear el estado del equipo.			
	Debe permitir la interacción a través de traps para integración con sistemas de monitoreo ²⁸			
	La solución debe contar con una herramienta de búsqueda de correos que permita ver el estado de cada correo procesado y que permita ver información a nivel forense, debe estar integrada al costo de la solución ²⁹			
Requerimientos de cumplimiento de Regulaciones internacionales	La solución debe contar con un engine para poder hacer cumplimiento con reglamentaciones como SOX, HIPPA, GLBA, PCI, etc. ³⁰			
	La solución debe contar con contenedores para identificadores de cada uno de los cumplimientos descritos y estos deben actualizarse de existir modificaciones a las regulaciones de forma automática			
	La solución debe contar con un repositorio de socios de negocio, que permita identificar a las empresas que precisan de ciertos cumplimientos ³¹			
	La solución debe contar con reglas que permitan parametrizar y ajustar cada uno de los cumplimientos en función de las necesidades de la empresa ³²			



²⁶ Ver Respuesta: N° 42 del Pliego de Absolución de Consultas y Observaciones

²⁷ Ver Respuesta: N° 43 del Pliego de Absolución de Consultas y Observaciones

²⁸ Ver Respuesta: N° 44 del Pliego de Absolución de Consultas y Observaciones

²⁹ Ver Respuesta: N° 45 del Pliego de Absolución de Consultas y Observaciones

³⁰ Ver Respuesta: N° 46 del Pliego de Absolución de Consultas y Observaciones

³¹ Ver Respuesta: N° 47 del Pliego de Absolución de Consultas y Observaciones

³² Ver Respuesta: N° 35 del Pliego de Absolución de Consultas y Observaciones

		Debe permitir la utilización de diccionarios específicos para cumplimientos de reglamentaciones locales o específicas. ³³			
		La gestión de políticas para la aplicación de las reglas de cumplimiento debe ser granulares. ³⁴			
		La solución debe contar con una sección específica de DLP en la cual se pueda ver un sumario de las violaciones a las políticas. ³⁵			
		Debe poseer folders específicos para identificación de violaciones, uno por cada política existente.			
		Debe contar con un área de búsqueda de incidentes que permita ubicar por distintos argumentos los mensajes.			
		Control de documentos clasificados ³⁶			
		La herramienta debe contar con un engine que permita identificar si algún documento clasificado como confidencial es enviado a través del correo, debe tener la capacidad de identificar el documento completo o partes del mismo			
		El engine debe poder ser configurado para solo permitir que usuarios autorizados envíen la información y debe poder tomar distintas acciones para las incidencias ³⁷			
		La solución debe poder almacenar los documentos en categorías, y los documentos deberán poder ser ingresados o de forma directa o a través de conexión con los resguardos definidos. ³⁸			
	Cifrado de correo	La solución debe contar con un engine que permita el cifrado de correos salientes			
		El cifrado debe ser transparente para los receptores, esto es no precisa de ningún tipo de agente en el sistema del receptor.			
		La gestión de las llaves debe ser provista en la nube, no debe depender del equipo emisor			
		La solución debe permitir al administrador revocar, delimitar en tiempo y eliminar usuarios lectores. ³⁹			
		La solución debe contar con un portal de autogestión para los receptores de correo cifrado.			
		La solución podrá funcionar sola o en combinación con las reglas definidas para el tráfico con el resto de los módulos.			
		Los correos cifrados emitidos deben poder ser vistos tanto en dispositivos móviles o aplicaciones como outlook.			



³³ Ver Respuesta: N° 36 del Pliego de Absolución de Consultas y Observaciones

³⁴ Ver Respuesta: N° 37 del Pliego de Absolución de Consultas y Observaciones

³⁵ Ver Respuesta: N° 38 del Pliego de Absolución de Consultas y Observaciones

³⁶ Ver Respuesta: N° 39 del Pliego de Absolución de Consultas y Observaciones

³⁷ Ver Respuesta: N° 48 del Pliego de Absolución de Consultas y Observaciones

³⁸ Ver Respuesta: N° 49 del Pliego de Absolución de Consultas y Observaciones

³⁹ Ver Respuesta: N° 50 del Pliego de Absolución de Consultas y Observaciones

		La herramienta debe poder permitir, de ser necesario, que los usuarios receptores puedan enviar correos a la corporación usando la misma herramienta.			
	Amenazas avanzadas	La solución debe contar con un módulo para amenazas avanzadas que permita identificar y contener las mismas si estas provienen a través del correo.			
		El módulo debe contar con un sandboxing para evaluar tanto archivos como urls para los archivos anexos, estos deben ser analizados a lo más en 5 minutos para el análisis de url's no solo debe ser capaz de ejecutar la mismas a través del sanboxing y poder identificar payloads en el sitio. Si al momento del análisis el sitio no se encuentra activo, el correo, de ser entregado, deberá contar con un mecanismo que proteja al usuario al hacer clic desde cualquier dispositivo que permita la navegación y este deberá hacer el análisis del site sin importar el número de clic's realizados por el receptor.			
		Debe mostrar a través de un dashboard la información relativa a los ataques recibidos, mostrar información forense de cada ataque y permitir ver quien ha sido el más atacado y quienes son los usuarios que regularmente hacen click a los links.			
	Recuperación de correos	La plataforma debe contar con un módulo, adicional y propietario, que permita la recuperación de correos que hayan cambiado su comportamiento una vez remitidos, debe poder automatizarse sobre todo con el módulo de amenazas avanzadas, es decir, la capacidad de retirar de los buzones correos que se haya detectado como malicioso posterior a su envío.			

CUMPLE: Indicar SI o NO

FOLIO: citar el folio donde se acredite

PARRAFO QUE SUSTENTE LA FUNCIONALIDAD: Copiar el párrafo que sustente la funcionalidad



ANEXO N° 02 de Estructura de Costos

Anexo 02 - Estructura de Costos

Servicio de seguridad para correo electrónico			
Item	Componente	Precio Unitario	Precio total
1	prestación principal		
1.1	Costo asociado a los componentes de hardware (servidor, consola de la solución u otros)		
1.2	Costo del licenciamiento de usuarios (total y unitario)		
1.3	Costo que corresponde al soporte de la solución (total y unitario)		
2	Costo de la prestación accesoria (Capacitación)		
Costo total de la solución ofertada			