

TÉRMINOS DE REFERENCIA

SERVICIO DE SOLUCIÓN ESPECIALIZADA EN PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM) PARA ELECTRO PUNO S.A.A

Área Usuaria:	Sub Gerencia de Tecnologías de la Información y Comunicaciones
Actividad del POI:	OEO14. Implementar Plan de Transformación Digital

1. OBJETIVO DE LA CONTRATACIÓN

Proveer a Electro Puno S.A.A una plataforma para la seguridad de correo electrónico institucional a fin de proteger en forma eficiente frente a las nuevas amenazas informáticas enviadas por correo, y de esta manera incrementar la disponibilidad de la comunicación por medio del correo electrónico institucional. Reforzar la Gestión de Seguridad de la Información en base a NTP 17001 ISO/IEC 27001. Esta solución deberá ser hosteada, es decir cloud.

2. FINALIDAD PÚBLICA

La finalidad de la presente contratación es la solución especializada en protección de correo electrónico (antispam), a fin de ofrecer protección ante las nuevas amenazas informáticas, Electro Puno S.A.A. envía y recibe correos electrónicos internos y de entidades a nivel mundial para las labores diarias y se necesita cubrir la necesidad tecnológica actual en seguridad y granularidad de seguridad de correo electrónico a fin de asegurar las nuevas tendencias informáticas actuales, permitiendo de esta forma aumentar la disponibilidad de la comunicación por este medio, y hacerle frente a las nuevas amenazas informáticas de correo.

3. MODALIDAD DE PAGO

Suma Alzada

4. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO

4.1 Suministro de un servicio de filtrado de correo electrónico para **269 usuarios**

ITEM	EQUIPO / SOLUCION	CANTIDAD DE BUZONES
1	SOLUCION ESPECIALIZADA EN PROTECCION DE CORREO ELECTRONICO (ANTISPAM)	269

El servicio suministrado debe ser compatible con los equipos existentes de Electro Puno S.A.A., para fines de integración, seguridad y soporte.

Una solución de Filtrado de contenido mail que cumpla con las siguientes características técnicas:

a) Premisas Generales

La solución cloud debe contar con la última versión liberada del software con que cuente el fabricante al momento de la entrega del sistema en operación.

- Debe ser una solución en nube (cloud) y de propósito específico.

- El esquema de comunicación debe ser seguro permitiendo únicamente el tráfico necesario para el servicio de correo y administración.
- Capacidad autónoma en servicios como DNS Cache para evitar dependencias en los DNS locales.
- Debe tener capacidad de evitar la recepción de correos por ataques de “bounce”, sin embargo, debe permitir el regreso de bounce legítimos.
- Se deberá de incluir todo lo necesario para la correcta operación de la solución.
- Debe proporcionar suficiente flexibilidad para adecuarse a diferentes topologías de red, así como responder a las necesidades de comunicación para envío y recepción de mensajes en diferentes escenarios.
- Las características enunciadas a continuación son mínimas, pudiendo ofertar una solución que supere los requerimientos solicitados.

b) Características mínimas

La solución deberá ser capaz de proporcionar los siguientes servicios:

- Esquemas de filtrado por reputación respaldado
- Filtrado Anti-Spam
- Protección Anti-Phishing
- Protección Anti-Virus
- Filtrado de Contenidos
- Mecanismos de autenticación
- Encriptación de medio de transferencia y de mensajes
- Debe soportar seguridad y control para la prevención de pérdida de datos
- Interoperabilidad con múltiples servicios de directorio, como Sun One o Sun iPlanet.
- Integración con múltiples plataformas de correo electrónico.

c) Características de Protección Anti-Spam y Filtrado de Contenido

- Se deberán incluir los algoritmos y métodos necesarios que permitan realizar una detección y filtrado de correo no deseado de calidad, además de reducir las detecciones falsas.
- Filtrado de correo entrante y saliente para los distintos niveles de filtrado.
- Filtrado por reputación de origen.
- Filtrado por análisis contextual de mensajes.
- Configuración de políticas por usuarios y grupos.
- Se debe incluir un mecanismo que permita analizar de manera automática todos los archivos adjuntos, detectar y eliminan de inmediato los archivos con software espía o virus, basados en regulaciones y por dominio, administración de incidentes y exploración continua de palabras clave, así como expresiones en todo el contenido de un mensaje incluyendo los archivos adjuntos.
- La tecnología Anti-Spam deberá proporcionar un alto grado de certidumbre, es decir, garantizar la eliminación de Spam para evitar falsos positivos.
- La solución Anti-Spam debe utilizar tecnologías de identificación precisas y minimizar el uso de esquemas heurísticos a lo estrictamente necesario y prescindir de ser posible de

métodos estadísticos como los esquemas bayesianos ya que requieren mucho mantenimiento y entrenamiento, además de la tendencia natural de dispersar en el tiempo su efectividad.

- Debe contar con un mecanismo especial para hacer la captura de spam en imágenes de forma efectiva.
- Se debe incluir una sólida protección contra esquemas "phishing" que se utilizan con frecuencia para obtener información confidencial sobre una organización o sobre usuarios individuales.

d) Características de Protección Anti-Virus y Hora Cero

- Antivirus (uno o múltiples engines).
- Análisis heurístico para identificación temprana de nuevos virus.
- Prevención de brotes (hora cero) de nuevos virus.
- Identificar y neutralizar virus antes de que puedan penetrar y propagarse en la red.
- Manejo de cuarentena por virus.
- Tecnología heurística que permita detectar las actividades propias de un virus, a fin de identificarlos y eliminarlos, aun siendo virus desconocidos. Debe ser posible ajustar la configuración de la heurística para obtener una identificación de virus agresiva.
- Debe contar con mecanismos de protección a fin de evitar ataques por DoS.

e) Características de Autenticación y Encriptación

- Debe soportar encriptación en el medio de transferencia de mensajes por TLS.
- Debe incluir herramientas que permitan realizar la autenticación del correo originado localmente por parte de los destinatarios utilizando un mecanismo como Domain Keys, DKIM o tecnologías semejantes que permitan identificar el uso de direcciones de remitente forjadas o "engañosas" en correos electrónicos.
- Contar con mecanismos que permitan validar destinatarios y evitar ataques de Directory Harvesting.
- Proporcionar algún esquema de encriptación de contenidos para el envío seguro de correos integrada a la solución.

f) Características de Administración y Reporteo

- Los accesos requeridos a la solución cloud deben ser bien por una consola propia vía comunicación serial, bien por acceso remoto por la red, pero solamente utilizando protocolos seguros: http direccionado a https, https, ssh.
- Actualizaciones automáticas de nuevas reglas, las actualizaciones deben ser auto administrables para garantizar que la red posea protección integral y precisa aun cuando cambien los métodos de ataque, en todo momento.
- Debe permitir ver reportes en tiempo real y generar informes gráficos de diferentes índoles, por ejemplo, informes sobre los usuarios de correo electrónico más frecuentes, los destinatarios de correo no deseado más frecuentes, los emisores de correo no deseado más frecuentes, entre otras opciones.

- Debe permitir filtrar y proteger múltiples servidores de correo electrónico y múltiples dominios.
- Difusión de alertas por email, SNMP o algún otro método que permita el monitoreo de condiciones de excepción en el dispositivo.
- Debe contar con mecanismos que permitan identificar los destinatarios de correo adecuadamente de tal forma que se pueda prevenir ataques de directorio y cosecha de información de directorios (Directory Harvest Attack).
- Debe integrarse a LDAP, Open LDAP, MS Active Directory para la administración de políticas y manejo de cuarentenas.
- Debe permitir controles de tasa, que permitan detener los ataques de negación de servicio y los ataques de correo no deseado basados en diccionarios.
- Control de filtrado de correo electrónico entrante y saliente por usuario o de manera global. El usuario final puede determinar el bloqueo de direcciones de contenido que no le interesa recibir.
- Debe permitir la configuración de cuarentena para que los usuarios puedan revisar correos electrónicos dudosos para su posible liberación y eliminación. El usuario debe tener acceso directo a la cuarentena.
- Se debe contar con alguna herramienta que permita al usuario reportar falsos negativos, falsos positivos o virus.

g) Características de Soporte

- Soporte 7 x 24 x 365 telefónico y web.
- El fabricante debe contar con presencia en el país con ingenieros calificados.
- El fabricante deberá contar con un centro de investigación para identificar nuevas formas de amenazas que genere filtros para los mensajes que contengan material indeseable. La actualización de dichos filtros debe ser frecuente y automática.
- El fabricante deberá contar con un centro de control y monitoreo de amenazas y ofrecer soluciones avanzadas para la prevención de amenazas y alertas tempranas de diversa índole.

5. REQUISITOS DEL POSTOR

El Contratista para el cumplimiento del servicio deberá adecuarse a las políticas de Electro Puno S.A.A. en cuanto a brindar un servicio de calidad. Por lo cual, deberá ser Persona natural y/o jurídica, para ello deberá adjuntar:

- Registro Nacional de Proveedores-RNP vigente (Copia simple) y/o se validara vía sistema web
- Declaración jurada de Cumplimiento de Términos de Referencia
- Declaración Jurada sobre Prohibiciones e Incompatibilidades, de No Estar Inhabilitado y No Impedido de Contratar con el Estado

6. PLAZO DE SERVICIO

El plazo total del servicio será de **385 días calendarios**, comprendidos según siguiente detalle:

- a) **La entrega, instalación, configuración y puesta en producción de la solución:** será de **15 días calendarios** como máximo, computados desde el día siguiente de la aprobación del plan de trabajo el cual se presentará y aprobará dentro de los **05 días calendarios** siguientes a la notificación y confirmación del pedido de compra, como máximo.
- b) **La vigencia** de la protección de correo electrónico antispam será de **365 días calendarios**, computados desde el día siguiente de la puesta en producción de la solución implementada, validada mediante el Acta de entrega de la implementación.

7. ENTREGABLES

Los entregables comprenderá lo siguiente:

- a. El Plan de Trabajo para la Instalación e implementación de la solución ofertada (elaborado por el contratista), para la definición y despliegue del proceso de ejecución de los servicios que forma parte de la solución.
- b. El Plan de Mantenimiento Preventivo de la solución ofertada, emitido por El contratista deberá ser entregado a la finalización de la instalación, configuración y puesta en producción de la solución.
- c. Informe técnico final de Instalación, configuración y puesta en producción de la solución ofertada que el contratista deberá entregar al finalizar la implementación y antes de emitir el acta de garantías y finalización del proyecto, emitido por El contratista, con el siguiente detalle:
 - Arquitectura de la solución
 - Configuración y puesta en operación de la solución
 - Pruebas de Conectividad
 - Acta de garantías y finalización del proyecto
 - Licencias, manuales y tutoriales personalizados, de la solución implementada en Electro Puno S.A.A.
 - Manuales de reporte y escalamiento de incidentes SLA.

8. FORMA DE PAGO

Se efectuará **pago único**, previa conformidad de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de Electro Puno S.A.A.

Para el pago se requerirá:

- Informe de conformidad de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de Electro Puno S.A.A.
- Comprobante de pago
- Cuenta Bancaria CCI
- Vigencia de la Suscripción del servicio por 365 días calendarios

9. CONFORMIDAD DEL SERVICIO

La conformidad será otorgada por la Sub Gerencia de Tecnologías de la Información y Comunicaciones de Electro Puno S.A.A

10. OTRAS CONSIDERACIONES PARA EJECUCIÓN DE SERVICIO

10.1 EQUIPAMIENTO TECNOLÓGICO

La solución debe ser compatible con el siguiente equipamiento existente:

- Servidor HP DL 380
- Microsoft Exchange 2016 estándar
- Servidor Virtual con replica de Exchange a nivel de DAG
- Integración con Office 365
- Conectividad switches marca Cisco
- Switch Core Cisco
- Firewall Palo Alto

10.2 EQUIPAMIENTO REQUERIDO

- No se aceptará sistemas operativos de uso genéricos.
- Debe ser una solución en nube de última generación.
- Debe tener la última versión oficial de software de la solución.
- Ninguno de las soluciones ofertadas podrá estar listados en la página web del fabricante como listas de end-of-life y end-of-sale.

La solución debe ser transparente en su conectividad y funcionamiento, con los equipos existentes en la infraestructura de Electro Puno S.A.A.

10.3 Garantía

No corresponde

10.4 Clausula anticorrupción y anti soborno

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, representados legales, funcionarios, asesores o personas vinculadas a la entidad.

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, directamente 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 la entidad

10.5 Solución de controversia

En el caso de contratos menores, las partes pactan la conciliación como mecanismo de solución de las controversias.

10.6 Resolución del servicio por incumplimiento

Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

- a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.

- b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
- c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
- d) Por incumplimiento de la cláusula anticorrupción.
- e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
- f) Configuración de la condición determinación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

10.7 Gestión de riesgos

No corresponde

11. PENALIDAD POR MORA

En el caso de retraso injustificado en la ejecución de la prestación, se aplicará al contratista la Penalidad por cada día de atraso, de acuerdo a la siguiente formula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Valor de F	Para bienes y servicios		F = 0.40
	Para obras	Para plazos menores o iguales a sesenta días	F = 0.40
		Para plazos entre sesenta y uno a ciento veinte días	F = 0.25
		Para plazos mayores a ciento veinte días	F = 0.15
	Para consultorías de obras	Para plazos menores o iguales a sesenta	F = 0.40
Para plazos mayores a sesenta días		F = 0.25	
Monto y plazo se refieren:	<ul style="list-style-type: none"> • Al contrato • Al ítem • A la ejecución periódica a la prestación parcial 		

Se asignará al contratista una penalidad hasta por un monto máximo equivalente al diez por ciento (10 %) del monto del contrato vigente, acumulado dicho porcentaje o excedido este, Electro Puno S.A.A., podrá resolver el pedido de compra y/o similar. Para lo cual bastara con emitir una comunicación al contratista tal decisión.

12. PRESENTACIÓN DE PROPUESTA

La propuesta económica deberá contener obligatoriamente los siguientes documentos, en las consideraciones mencionadas y en el siguiente orden:

- Carta de Presentación
- Registro Nacional de Proveedores – RNP vigente (Copia simple) y/o se validara vía sistema web.
- Propuesta Económica (**Anexo 01**)

- Declaración Jurada de Cumplimiento Términos de Referencia y/o Especificaciones Técnicas (**Anexo 02**)
- Declaración Jurada sobre Prohibiciones e Incompatibilidades, de No Estar Inhabilitado y No Impedido de Contratar con el Estado (**Anexo 3**)

IMPORTANTE: Para la presentación de expediente deberán tener en consideración los siguientes puntos:

- El expediente deberá estar debidamente **Foliado** correlativamente.
- El expediente deberá ser remitido en un **solo archivo PDF**
- De presentar de forma física, el expediente deberá ser remitido en sobre cerrado.
- La documentación consignada tiene carácter de declaración jurada, por lo que el postor será responsable de la información consignada en dichos documentos y se somete al proceso de verificación posterior de la entidad.
- Los anexos del presente proceso se encuentran en la PAGINA WEB INSTITUCIONAL <https://www.gob.pe/institucion/electropuno/colecciones/17937-servicios-de-terceros>

NOTA: FAVOR DE ENVIAR SU COTIZACIÓN Y TENER EN CUENTA LO SIGUIENTE:

Para que sea considerada una oferta válida y poder participar en la presente convocatoria, es necesario y obligatorio presentar por una de estas modalidades:

- **OPCIÓN 01:** Mesa de partes, sito en Jr. Mariano H. Cornejo N° 160 – Puno, en sobre cerrado, y/o
- **OPCIÓN 02:** Mesa de partes virtual: <https://wselpu.electropuno.com.pe/sgdVirtual/1>

Electro Puno S.A.A.