BASES

EXONERACION Nº 002-2017-AGROBANCO

ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB

EXONERACION N° 001-2017-AGROBANCO

CAPÍTULO I

GENERALIDADES

1.1 ENTIDAD CONVOCANTE
Nombre : Banco Agropecuario - AGROBANCO
RUC N° : 20504565794

1.2 DOMICILIO LEGAL
Av. República de Panamá N°3531 Dpto. 901, San Isidro, Lima

1.3 OBJETO DE LA CONVOCATORIA
El presente procedimiento tiene por objeto la **ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB.**

1.4 VALOR REFERENCIAL TOTAL: El valor referencial asciende a **S/ 59,980.00 (Cincuenta y Nueve Mil Novecientos Ochenta con 00/100 Soles)**, incluido los impuestos de Ley y cualquier otro concepto que pudiera incidir en el costo total del servicio. El valor referencial ha sido calculado al mes de marzo del año 2017.

DESCRIPCIÓN DEL SERVICIO	VALOR REFERENCIAL
ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB	**S/ 59,980.00** (Cincuenta y Nueve Mil Novecientos Ochenta con 00/100 Soles)

El expediente de contratación fue aprobado mediante documento de fecha **29 de marzo de 2017.**

1.5 FUENTE DE FINANCIAMIENTO
Recursos Directamente Recaudados.

1.6 SISTEMA DE CONTRATACION
El presente proceso de selección se rige por el sistema de suma alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.7 BASE LEGAL

- Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros y AFP.
- Ley N° 27603, Ley de Creación del Banco Agropecuario
- Ley N° 29064, Ley de Relanzamiento del Banco Agropecuario
- Ley N° 29523, Ley de Mejora de la Competitividad de las Cajas Municipales de Ahorro y Crédito del Perú
- Ley N° 29596, Ley que viabiliza la ejecución del Programa de Re-estructuración de la deuda agraria (PREDA) y complementarias.
- Directiva de Gestión y Proceso Presupuestario de las Empresas bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE)
- El Reglamento de Adquisiciones y Contrataciones de AGROBANCO que se encuentra publicado en la página web del Banco.

CAPITULO II
ETAPAS

2.1 CRONOGRAMA

- Convocatoria..... : 29/03/2017
- Registro de Participantes.....: 30/03/2017
- Presentación de Propuestas.....: 30/03/2017
  Lugar: Av. República de Panamá 3680 4to piso
- Calificación de Propuestas.....: 30/03/2017
- Adjudicación..... : 30/03/2017

2.2 REGISTRO DE PARTICIPANTES

El registro de los participantes se realizará de **manera gratuita** y previa a la presentación de propuestas en la Oficina Administrativa de AGROBANCO, Av. República de Panamá 3680 4to. Piso, hasta las 17:00 horas adjuntándose copia de su RNP (Bienes).

2.3 PRESENTACION DE PROPUESTAS

Las propuestas se presentarán en dos sobres cerrados y estarán dirigidas al Departamento de Logística, conforme al siguiente detalle:

Señores
AGROBANCO
Att.: Departamento de Logística
EXONERACIÓN N° 002-2017- AGROBANCO
ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB
SOBRE N° 1: PROPUESTA TÉCNICA
NOMBRE / RAZON SOCIAL DEL POSTOR

Señores
AGROBANCO
Att.: Departamento de Logística
EXONERACIÓN N° 002-2017- AGROBANCO
ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB
SOBRE N° 2: PROPUESTA ECONOMICA
NOMBRE / RAZON SOCIAL DEL POSTOR

Todos los documentos que contengan información esencial de las propuestas se presentarán en idioma castellano, o en su defecto, acompañados de traducción oficial, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que podrá ser presentada en el idioma original. El postor será responsable de la exactitud y veracidad de dichos documentos.

Los formatos podrán ser llenados por cualquier medio, incluyendo el manual, debiendo llevar el sello y la rúbrica del postor o su representante legal o mandatario designado para dicho fin.

2.3.1 Contenido de las Propuestas

Se presentará un (1) original.

SOBRE Nº 1 - PROPUESTA TECNICA:

Documentación de presentación obligatoria:

1. Copia simple de la constancia vigente de inscripción en el Registro Nacional de Proveedores: Registro de Proveedores de **Bienes**.
2. **Anexo Nº 01 -** Declaración Jurada de datos del postor.
   Cuando se trate de consorcio, esta declaración jurada será presentada por cada uno de los consorciados**.**
3. **Anexo Nº 02 -** Declaración jurada en la que el postor declare que su oferta cumple las Especificaciones Técnicas contenidas en el **Capítulo III** de las Bases.
4. **Anexo Nº 03 -** Declaración jurada en la que se compromete a mantener la vigencia de la oferta hasta la emisión de la orden de compra.
5. **Anexo Nº 04 -** Declaración jurada de plazo de entrega.

SOBRE N° 2 - PROPUESTA ECONOMICA:

1. Contendrá el monto total de la propuesta económica en soles **(Anexo Nº 05),** incluidos todos los tributos, seguros, transportes, conforme a la legislación vigente, así como cualquier otro costo que pueda tener incidencia sobre el costo del servicio.

2.4 CALIFICACION DE PROPUESTAS

Se evaluará el cumplimiento de los términos de referencia contenidos en el Capítulo III de las presentes bases. La propuesta que no cumpla dicho requerimiento no será admitida.

2.5 ADJUDICACION

La Adjudicación se registrará en la página web de la entidad en la fecha prevista en el cronograma.

2.6 REQUISITOS PARA LA EMISIÓN DE LA ORDEN

a) Copia de DNI del Representante Legal.
b) Copia de la vigencia del poder del representante legal de la empresa no mayor a sesenta días de antigüedad.
c) Copia de la constitución de la empresa y sus modificatorias debidamente actualizado.
d) Copia del RUC de la empresa.
e) Código de Cuenta Interbancario (CCI), de corresponder.

2.7 CONFORMIDAD

La conformidad estará a cargo de la Gerencia de Desarrollo de AGROBANCO.

2.8 PLAZO PARA EL PAGO

La Entidad se compromete a efectuar el pago al contratista en un plazo máximo de 10 días calendario de otorgada la conformidad de recepción de la prestación.

2.9 FORMA DE PAGO

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

- Factura
- Presentación conformidad del área usuaria.

El pago será único al final del servicio, a través del abono directo en cuenta del proveedor.

CAPÍTULO III

ESPECIFICACIONES TÉCNICAS

Objeto: ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

I. OBJETO

AGROBANCO, a través del área de Sistemas, requiere la "ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD", que permita contar con soluciones de antivirus corporativo, filtro de correos (antispam) y filtro de páginas web, de acuerdo a las especificaciones técnicas que se detallan en el presente documento.

II. REQUISITOS QUE DEBERA CUMPLIR EL POSTOR

- El proveedor deberá estar inscrito en el Registro Nacional de Proveedores del Organismo Supervisor de las contrataciones del Estado, cuando se trate de un proceso de selección.
- El proveedor no deberá estar inhabilitado para contratar con el estado peruano.
- El proveedor debe tener más de 03 años de experiencia en el Perú implementando soluciones de antivirus, filtro de contenidos y filtro de correos de la marca ofertada.
- El proveedor deberá brindar garantía y soporte de los bienes suministrados, por el plazo de 1 año.

III. CARACTERÍSTICAS TÉCNICAS DEL BIEN

El postor deberá realizar la Instalación, configuración y/o actualización de las siguientes soluciones de seguridad:

Solución de seguridad – 700 licencias por 12 meses:

- Setecientos (700) licencias de seguridad para Endpoint
- Setecientos (700) licencias de seguridad para Filtro de Mensajería
- Setecientos (700) licencias de seguridad para Filtro de Contenidos

3.1. Solución de seguridad – 700 licencias por 12 meses

El postor deberá considerar una solución de seguridad para 700 licencias para la entidad.

Las características de cada módulo de seguridad son las siguientes:

a) Setecientos (700) licencias de seguridad para Endpoint

La solución antivirus debe proteger a los siguientes sistemas operativos, puestos de trabajo fijos y móviles (portátiles) en las plataformas Intel y AMD, los sistemas operativos: Windows 7, Windows vista, Windows 8, Windows 8.1 y posteriores.

La solución de antivirus para la protección de puestos de servicios debe contar con al menos las siguientes capacidades de protección:

Protección Web

- La solución de antivirus, deberá contar con un sistema basado en la reputación de sitios web del fabricante de la solución, que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
- El sistema de manejo de la reputación de archivos deberá estar integrado en la misma consola de antimalware como parte de la misma solución.
- De manera independiente el sistema de reputación de sitios web podrá implementarse por separado y poder integrarse a la consola de antimalware.
- Manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro de la red corporativa
- Manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran fuera de la red corporativa
- Permitir reclasificar sitios web
- El sistema de protección Web no deberá depender de ningún explorador en específico.
- Permitir editar la lista de URL para permitir acceso a URL´s que se encuentran bloqueadas (razón sitio de mala reputación o interna) a nivel general, grupos o personal.

Protección contra infecciones de malware

- Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
- Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
    - Procesos que se ejecutan en la memoria principal (RAM)
    - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
    - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
    - Archivos recibidos a través de software de comunicación instantánea (MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
    - Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
    - La detección heurística de virus desconocidos.

Métodos de escaneos

- Manejar un sistema basado en distribución de firmas de malware desde la consola principal hacia las estaciones de trabajo. (método convencional).
- Manejar un sistema adicional de consulta de firmas de malware basado en reputación de archivos. Utilizando tecnología de Cloud Computing.

- La consola de antimalware podrá administrar los dos métodos de disponibilidad de firmas a todas las estaciones de trabajo reportadas en la consola, por grupo o por estación de trabajo.
- La consola de antimalware permitirá ver el estado de la consola que administra las firmas basadas reputación de archivos.
- En la consola se podrá ver estatus de las estaciones de trabajo que se encuentran operando en un modo convencional o en modo basado en firmas en la nube y que se encuentran en línea o fuera de línea.
- El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera integrada y visualizada desde la misma consola de antimalware.
- El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera independiente (stand alone) y visualizada desde la misma consola de antimalware.
- Manejar actualizaciones incrementales tanto del servidor a la nube, como del servidor a los clientes sin que estás sobrepasen de 100K.

Control de dispositivos

- Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas.
- La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario tenga un control total sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario únicamente tenga permisos de solo lectura sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir que el usuario tenga únicamente permisos de lectura y ejecución sobre el dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger
- Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá evitar que el usuario pueda tener acceso al contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger

Reporte de amenazas a los laboratorios.

- Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
- Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.

Utilización de CPU

- Selección del nivel de utilización de CPU mientras se realiza un escaneo Programado, manual o desde la consola.

- La solución de antimalware podrá manejar niveles de uso del CPU cuando el usuario ejecute un escaneo manual, dicha configuración deberá manejarse de manera centralizada por el administrador.
- La solución de antimalware podrá manejar niveles de uso del CPU cuando se programen los escaneos a las estaciones de trabajo, dicha configuración deberá manejarse de manera centralizada por el administrador.
- La solución de antimalware podrá manejar niveles de uso del CPU cuando el usuario ejecute desde la consola de antimalware, dicha configuración deberá manejarse de manera centralizada por el administrador.

Informe de cumplimiento
- Garantizar que los clientes tengan los servicios activos, últimos componentes, consistencia en configuraciones y que han corrido escaneos regularmente.

Administración
- La solución debe garantizar la seguridad a través de SSL para las comunicaciones entre el servidor y la dirección web de la consola;

Login
- Integración con Active directory para la asignación de roles y permisos de Acceso a las configuraciones de la consola.

Resumen de sistema
- Visualizar, de forma rápida y sencilla, el estado de las estaciones de trabajo y servidores en una sola pantalla de Summary.
- Visualizar, de forma rápida y sencilla, el estado y estadísticas de las infecciones generadas y permitir también visualizar las estaciones de trabajo y servidores donde ocurrió la detección o infección.
- Visualizar, de forma rápida y sencilla, un resumen del estatus de las actualizaciones de firmas en las estaciones de trabajo y servidores, cantidad de equipos actualizados y desactualizados.

Manejo de grupos
- Agregar, modificar o eliminar Grupos para administración de los clientes con políticas diferentes

Logs
- Petición de Log de amenazas, actualizaciones y estado del servidor.

Configuraciones
- Aplicar configuración de políticas por servidor o estación de trabajo, por grupo o por usuario de manera independiente.
- Manejo de configuraciones
- Importar o Exportar configuraciones de políticas de un grupo de estaciones de trabajo a otro.
- Habilitar o deshabilitar el firewall de acuerdo a la ubicación física de usuario así como personalización de las políticas o excepciones.
- Lanzar una política de seguridad en caso de epidemias.
- Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.

- Personalizar los permisos de los clientes para realizar acciones en el software local.
- Petición de Actualización de patrones, configuraciones y software de forma inmediata.
- Lanzamiento de escaneos manuales a unidades del sistema o archivos mediante la consola del cliente o la navegación del explorador de Windows.
- Visualización Inmediata de los logs generados en los diferentes componentes de la solución.
- Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.

Clientes fuera de la red
- Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

Integración con Active Directory
- Integración de la solución con un dominio de Active Directory.
- Permitir la integración con Active Directory aún si el equipo en donde se instalará una consola de administración antivirus no se encuentra en el dominio.
- Permitir generar un análisis, listado de equipos que cuenten o no con una protección antimalware, basado en dominios o grupos del Active Directory.
- Apoyar múltiples dominios de confianza y los bosques de Active Directory;
- Utilizar la clave de cifrado antivirus que se encuentren en conformidad con Active Directory para realizar una conexión segura entre el servidor y el controlador de dominio de antivirus;
- Permitir a los clientes del árbol de directorios del antivirus, sea un reflejo del árbol de directorios de Active Directory.

Administración centralizada
- La solución antivirus debe poseer una consola de administración centralizada a la cual debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia.

Instalación clientes
- Paquete de instalación. Integración de la solución con un dominio de Active Directory.
- Consola Web. Instalación de cliente antivirus mediante la URL de la Consola de la solución.
- Línea de comandos. Instalación de cliente antivirus mediante línea de comandos o script.
- Remoto. Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
- Active Directory. Lanzamiento de instalación vía integración con el dominio de Active Directory.
- Segmentos de red. Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
- Desinstalado automático. Desinstalación automática de otras soluciones para la instalación del cliente antivirus.

Desinstalación de clientes
- Manual. Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
- Remoto. Desinstalación del cliente de forma remota desde la consola de administración.

Actualización del servidor
- Manual. Petición de Actualización de patrones del servidor de forma manual.

- Automática. Configuración de Actualizaciones automáticas, así como la fuente de actualización.

Actualizaciones de clientes

- Manual y automáticamente desde consola. Distribución de actualizaciones a los clientes de manera Automática y Manual.
- Cliente sin conectividad al servidor. Actualización de sistema de firmas para clientes sin conectividad al servidor.
- Active Update. Actualización de grupo de usuarios por Agentes de Actualización o repositorios.

Consolidación de consolas de administración antivirus (Administración central)

- La solución deberá contar con una herramienta que consolide la administración de todas las consolas antivirus que se instalen.
- La consola de administración central deberá poder desplegar el licenciamiento a las demás consolas antivirus.
- La consola de administración central deberá ser el repositorio de logs y actualizaciones de todas las consolas antivirus.
- La consola central de administración deberá permitir replicar configuración.
- La consola central de administración deberá permitir y programas reportes consolidados.
- La consola de administración centralizada debe tener la capacidad de ser consultada mediante navegador web desde cualquier estación de trabajo que cuente con MS Internet Explorer.
- La consola debe permitir la creación de diversos usuarios para su administración y con diferentes niveles de acceso.
- La consola de administración centralizada debe tener la capacidad de notificar los intentos de infección de virus de acuerdo a parámetros definidos por el administrador de la solución.
- La consola de administración centralizada debe poseer la capacidad de actualizar las políticas de seguridad desde el fabricante en caso de una epidemia mundial de virus informativos.
- La consola de administración deberá de permitir características de administración proactiva para brindar a los administradores información y recomendaciones de políticas antes de la generación de patrones de virus. Políticas contra epidemias de virus
- La consola deberá permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre la solución de seguridad.
- Debe ofrecer administración centralizada de las consolas de los productos de antivirus de las diferentes capas de protección.
- Distribución automática y/o programada de actualizaciones para los distintos productos de antivirus desde cada 5 minutos.
- Reportes centralizados de incidencias de virus en distintos productos y plataformas de la misma suite de antivirus, generando estadísticas y análisis.
- Despliegue de políticas preventivas /reactivas para código malicioso en casos de alerta.
- Detección de amenazas asociadas con virus y software malicioso.
- Servicios de limpieza de daños en tiempo real y libre de agente para eliminar remanentes de virus, troyanos, sypware y entradas en el registro del sistema.
- Notificación inmediata y centralizada sobre ataques masivos de virus y/o código malicioso.
- El producto deberá soportar Instalación Local desde un CD, Conexión a red, etc.

Control de aplicaciones

- Para la prestación del Servicio de protección contra código malicioso en puestos de servicio se debe considerar una solución que evite que aplicaciones no autorizadas o maliciosas se ejecuten en los puestos de servicio.

b) Setecientos (700) licencias de seguridad para el Filtro de Mensajería

Para la protección del filtro de mensajería se requiere una solución que cumpla las siguientes características mínimas:

- Deberá poder instalarse sobre ambientes físicos o equipos virtuales vmware ESXi.
- Deberá estar basada en un sistema operativo de 64 bits.
- Deberá poderse implementar en esquemas de Alta Disponibilidad, dónde un equipo sea el responsable de la centralización de bitácoras y configuración de todos los equipos que forman parte de la arquitectura en Alta Disponibilidad.
- Deberá contar con actualizaciones para sus patrones y motores de detección de spam (en imágenes y heurística), phising y código malicioso.
- Deberá basarse en la comparación de la calificación final del correo después de ser analizado contra un umbral que podrá ser configurado.
- Deberá detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del Fabricante, permitiendo la configuración de umbrales para esta detección y la acción a tomar.
- Deberá soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Deberá revisar tanto el correo entrante como el saliente.
- Debe ofrecer capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Debe ofrecer el análisis de archivos comprimidos en los formatos más populares con 7 capas de compresión.
- Debe detectar el verdadero formato de un archivo sin basarse en el nombre, extensión o tipo MIME del mismo y poder aplicar acciones personalizadas ante su detección.
- Debe contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos de Microsoft Office, Adobe PDF y archivos de texto.
- Debe poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP como en políticas cuando el correo ya ha sido recibido.
- Debe ser capaz de recibir tráfico con conexiones TLS y poder hacer conexiones con otros servidores de TLS.
- Deberá contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- 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). Para esto, es necesario que la solución pueda integrarse con múltiples servicios de directorio como Active Directory y OpenLDAP de forma simultánea y en múltiples dominios.

- Deberá contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen el dominio destino (correos de rebote o Bounced Mails).
- Deberá hacer un bloqueo automático de IPs debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- Deberá ser capaz de poder configurarse de tal forma que pueda haber excepciones, tanto en hosts remitentes como en destinatarios para asignar políticas diferentes.
- Deberá permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
- Deberá permitir la creación de políticas a nivel global por grupos o por usuario.
- Deberá de realizar la actualización de firmas de spam y códigos maliciosos en periodos configurables.
- Deberá contar con un método de respaldo de configuración de la solución.
- Deberá permitir el manejo de múltiples dominios, al menos 50 diferentes, para la limpieza de correo de spam y código malicioso.
- Deberá contar con protección anti-relay para correo de entrada o de salida basada en dominios, cuentas de correo y direcciones IP.
- Deberá contar con un método de revisión de mensajes en cuarentena basada en consultas, por remitente, asunto, destinatario y que permita revisar archivos adjuntos y cuerpos de mensaje, en formato texto.
- Deberá contar con sistema de revisión de logs de entrada y salida de tráfico de correo que permita realizar búsqueda de palabras, para su consulta rápida.
- Deberá poder, a solicitud de la Institución, almacenar el correo rechazado de forma temporal en la nube, por al menos 24 horas antes de ser eliminado.
- Deberá contar con tecnología heurística que permita detectar las actividades propias de un código malicioso, a fin de identificarlos y eliminarlos, aun siendo códigos maliciosos desconocidos. Además deberá poder proporcionar recomendaciones sobre la acción a tomar ante diferentes tipos de malware.
- Capacidad para evitar la fuga de información confidencial basada en expresiones regulares y palabras clave.
- Capacidad para evitar la fuga de información a través de plantillas predefinidas.
- Capacidad de detección de amenazas avanzadas y ataques dirigidos, a través del análisis automatizado de archivos adjuntos de correo electrónico en un ambiente de sandbox, el cual debe estar implementado en la infraestructura de la institución, no se aceptan sandbox de nube.
- El servicio deberá contar con la programación de reportes basados en plantillas para ser generados en períodos configurables con tablas y gráficos, y poder ser visualizados desde la consola de administración de la solución.
- El fabricante de la solución deberá contar con centros especializados en la investigación de amenazas
- La solución para la protección de correo electrónico externo debe tener capacidad para evitar la fuga de información confidencial basada en la detección de palabras clave (keyword) y expresiones regulares por protocolo SMTP.
- La solución debe tener la capacidad de integrarse a una consola central de administración, desde la cual se puedan administrar otras soluciones como la solución para la protección de la navegación web, antivirus y se puedan aplicar políticas para evitar la fuga de información confidencial desde un punto central tanto en el Gateway como en el endpoint.

c) Setecientos (700) licencias de seguridad para el Filtro de Contenidos Web

La solución propuesta por para brindar el presente servicio, deberá contar con las siguientes características tecnológicas:

- Deberá poder instalarse sobre ambientes físicos o equipos virtuales vmware ESXi y hyper-v montado sobre servidores Windows 2008 R2 y Windows Server 2012.
- La base de datos de categorías de la solución debe estar en la nube y poder ser consultada en tiempo real, no depender de actualizaciones o descargas locales para mejorar el nivel de la categorización.
- La solución debe contar con un mínimo de 82 categorías para filtrado de URLs
- La solución debe permitir la creación de categorias personalizadas de URL's, indicando la URL del sitio, dominio, palabras claves o una frase que identifique la URL del sitio.
- La solución debe permitir tomar acciones para URL's que aún no se encuentren categorizadas.
- Filtrado de URLs no productivas para el negocio, uso apropiado y disponibilidad del ancho de banda
- Filtrado de URLs maliciosas para incrementar la seguridad
- Filtrado de scripts maliciosos, objetos y contenido web
- Debe tener la capacidad de escaneo de malware en protocolos HTTPS
- Debe tener la capacidad de filtrado por categoría en protocolos HTTPS
- Capacidad de brindar la protección en tráfico HTTP, HTTPS y FTP.
- Permitir el manejo de la herramienta vía Web (HTTP o HTTPS).
- Para el filtrado por categoría la solución debe contar con al menos las siguientes acciones, monitoreo, bloqueo, cuotas de tiempo, acceso a categorías restringidas cuando el usuario proporcione un password definido por el administrador y notificar al usuario para permitir que el usuario elija continuar con el acceso al sitio o desistir.
- La solución debe tener la capacidad de aplicar filtros basados en el contenido de los headers del protocolo HTTP, y aplicar filtros que permitan limitar el uso de cierto tipo de navegadores identificándolos por el user agent, limitar el tamaño de los archivos que son subidos a sitios en internet, evitar que se hagan consultas de ciertas palabras en buscadores, evitar que se hagan post a sitios web y permitir solo la visualización del sitio, etc.
- Aceleración de tráfico mediante el uso de caching
- Monitoreo y reporteo
- La solución debe soportar el manejo del header X-Forwarded-for.
- La solución debe contar con la funcionalidad de control de aplicaciones, la cual debe permitir o bloquear la aplicación indicada, debe controlar un mínimo de 800 aplicaciones.
- Infraestructura global de bloqueo de páginas maliciosas basada en la reputación de seguridad de la misma
- Permitir la creación de políticas de control de accesos por día, por horario laboral y días específicos.
- Poseer características que permitan la consulta o recepción de nuevos patrones de seguridad de las siguientes formas:
- A partir de la consola Web, por medio de un sitio del fabricante del producto en Internet:
    - Descarga de paquetes incrementales.
    - Descargas programadas.
    - Descargas bajo demanda solicitadas manualmente.

- Deberá tener la capacidad de analizar y contener amenazas que puedan ser parte de un ataque dirigido.
- Deberá tener la capacidad de bloquear descargas por tipo de extensión de archivo.
- Deberá contar con la funcionalidad de detección, eliminación y prevención de amenazas y códigos maliciosos en tiempo real.
- Deberá poseer la característica de detección de virus, spyware, grayware, phishing, worms, troyanos y demás códigos maliciosos.
- Deberá contar con la característica de detectar código malicioso a través de patrones y/o heurística.
- Qué posea la característica de detección de tráfico malicioso proveniente de una botnet o el intento de comunicación desde un cliente de la red a una botnet y pueda controlarlo.
- Poseer las características de identificación y eliminación de código malicioso como consecuencia del acceso a las páginas Web con contenido de applets de Java, ActiveX, etc.
- Facilitar el almacenamiento de eventos (logs) del acceso de los usuarios a través de HTTP y FTP, así como también de códigos maliciosos encontrados a fin de hacer una investigación en el registro sin necesidad de utilizar herramientas de terceros, y generar informes consolidados.
- Poseer características que hacen respaldos de la configuración actual y restaurar la configuración del producto.
- Tener la capacidad de manejar el aislamiento para los archivos con malware o no reparables en áreas de cuarentena.
- Interactuar con servidores LDAP como Windows Active Directory y/o con Open LDAP.
- Posibilidad de instalarse en los siguiente modos: Transparent Bridge, ICAP server, Forward Proxy, Transparent usando WCCP y Reverse Proxy.
- Tener la capacidad escanear contenido HTTP y FTP de clientes que suben o descargan contenido a un servidor Web, protegiéndolo de amenazas.
- Tener la capacidad de integrarse con otros dispositivos proxy como (bluecoat y squid) para complementar la seguridad de la Institución.
- Ofrecer Alta Disponibilidad en modo Transparente Bridge.
- Integración con dispositivos ICAP como complemento a la seguridad de la Institución.
- Poseer el método de bloqueo de las descargas por tipo de archivo.
- Filtrado de URLs maliciosas a través de políticas por grupos de usuarios, IPs o grupos en el Directorio Activo.
- Filtrado de scripts maliciosos, objetos y contenido Web.
- Aceleración de tráfico mediante el uso de caché, para reducir la carga en los servidores y el consumo de ancho de banda.
- Los servidores de esta solución, deberán contar con acceso a Internet, de tal forma que se puedan conectar a los sitios del fabricante para alimentar las bases de datos de reputación y para obtener información de ellas para la consulta de sitios maliciosos.
- Se deberá tener la capacidad de inspeccionar trafico HTTP a través de sentencias o comandos integrados en los encabezados del paquete, permitiendo o bloqueando su ejecución
- Capacidad de validar la vigencia, autenticidad de certificados de sitios HTTPS
- Capacidad para evitar la fuga de información confidencial basada en expresiones regulares y palabras clave.
- Capacidad para evitar la fuga de información a través de plantillas predefinidas.
- Capacidad de detección de amenazas avanzadas y ataques dirigidos, a través de la integración automatizada con un sanbox para análisis de archivos en un ambiente de simulación local que resida en la infraestructura del cliente.

- La solución debe contar con un motor de escaneo de malware que tenga la capacidad de detectar malware tradicional, pero también cuente con capacidades de heurística para detectar amenazas nuevas.
- La solución debe contar con la capacidad de detectar y evitar la fuga de información confidencial a través de web, basándose en la identificación de información confidencial por palabras claves, y expresiones regulares.
- Debe contar con plantillas para la detección de información confidencial como mínimo PCI/DSS, SB-1386, GLBA.
- La solución debe verificar la fuga de información confidencial por protocolo FTP.
- La solución debe tener la capacidad de integrarse a una consola central de administración, desde la cual se puedan administrar otras soluciones como la solución para la protección de correo externo, correo interno, antivirus y se puedan aplicar políticas para evitar la fuga de información confidencial desde un punto central tanto en el Gateway como en el endpoint.

3.2. Instalación y puesta en producción

El servicio de instalación y configuración de la solución ofertada estará a cargo del postor y será llevado a cabo dentro de la zona de Lima Metropolitana.

3.3. Mantenimiento y Soporte técnico 24x7

Referente a toda la solución, se debe incluir el Servicio de Soporte y 02 Mantenimientos Preventivos al año (semestral) y Mantenimiento Correctivo por 01 año bajo la modalidad 24x7x365 (Lunes a Domingo) y un tiempo de respuesta no mayor a 2 horas, iniciándose ambos a partir de la firma de contrato bajo las siguientes condiciones:

a) El tiempo de respuesta deberá no ser mayor a 2 horas y un tiempo de resolución máximo de 8 horas.
b) Los servicios de mantenimiento correctivo de las soluciones deberán estar disponibles sin límite de horas por intervención, ni cantidad de intervenciones mensuales del personal del proveedor; dándose por atendido un problema cuando es solucionado en su totalidad.
c) El personal técnico del proveedor, para solucionar un problema o incidente reportado, deberá apersonarse a las instalaciones de AGROBANCO, salvo que previamente y por mutuo acuerdo entre el personal técnico de ambas partes, se convenga que dicho soporte sea telefónico.
d) El postor proveerá información del estado del problema reportado.
e) Para situaciones que se pueden calificar como críticas, el proveedor deberá generar un procedimiento alternativo para evitar el problema o una solución temporal de parche en espera de una solución definitiva.
f) No podrá modificarse el nivel, calidad, periodicidad, categoría o cualquier otra característica de estos servicios durante el período de garantía, sin consentimiento de AGROBANCO.
g) Mano de obra y repuestos para cualquier servicio de atención por hardware.
h) Mantenimiento preventivo cada seis (06) meses en las instalaciones de AGROBANCO, en horario a coordinar con personal de Sistemas de AGROBANCO.
i) El Postor deberá contar con un centro de atención de requerimientos de servicios, de reparación o asistencia técnica o mesa de ayuda, de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con los servicios estipulado en las bases durante todo el tiempo de la garantía este servicio debe estar disponible 24x7x365.

Mantenimiento correctivo cada vez que se presente una falla o mal funcionamiento propio de la solución

3.4. Requerimiento de Personal

El postor deberá de contar con el siguiente personal técnico calificado:

Instalación de los productos ofertados

- **Licencias de seguridad para Endpoint:** Dos (02) Ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

- **Licencias de seguridad para Filtro de Mensajería:** Dos (02) Ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

- **Licencias de seguridad para Filtro de Contenidos:** Dos (02) Ingenieros y/o técnicos de telecomunicaciones, sistemas o afines; certificados en los productos ofertados. Adjuntar copia de certificados de estudios y certificados emitidos por el fabricante.

Mesa de ayuda y Soporte Post Venta

Un (01) Ingeniero y/o técnico de las especialidades de Ingeniería Electrónica, Sistemas o Telecomunicaciones o a fines, con Certificación ITIL y con certificación en una de las soluciones de endpoint.

- Mínimo Tres (03) personas especialistas con certificación emitida por la marca solución ofertada.
- Declaración Jurada Simple sobre los ingenieros y/o técnicos que se presenten como personal certificado por el fabricante ofertado, se encuentre en planilla de la empresa postora como trabajadores, no se aceptará personal que esté en modalidad de prestación de servicios, para dicho efecto además se deberá adjuntar la consulta RUC en la web de la SUNAT respecto de la Cantidad de Trabajadores y/o Prestadores de Servicio.

Capacitación de los productos ofertados

El Postor deberá realizar una capacitación de los productos ofertados con un total de doce (12) horas. El detalle de los cursos es el siguiente:

- Curso cuatro (04) horas para soluciones de seguridad de endpoint. El instructor deberá estar certificado por el fabricante en soluciones de seguridad para endpoint.
- Curso cuatro (04) horas para soluciones de filtro de mensajería. El instructor deberá estar certificado por el fabricante en soluciones de filtro de mensajería.
- Curso cuatro (04) horas para solución de filtro web. El instructor deberá estar certificado por el fabricante en soluciones de filtro web.

El postor en su propuesta, deberá indicar la marca y nombre de las soluciones ofertadas, así mismo deberá adjuntar la hoja de datos (datasheet) de cada solución presentada.

El postor deberá ser partner de los productos ofertados. Deberá adjuntar carta del fabricante con referencia al proceso indicando dicho partnership. Se deberá indicar además en la carta el nivel de partner que el fabricante le asigna.

3.5. Garantía

La garantía del postor por las soluciones que componen la oferta deberá ser por un año. Esto cubre el soporte de software y el derecho a contar con la última versión de las soluciones ofertadas por los fabricantes durante la duración del contrato.

3.6. Condiciones Finales

- El postor en su propuesta deberá indicar la marca y versiones de las propuestas ofertadas, así mismo deberá adjuntar el documento técnico (datasheet) de cada propuesta presentada.

- El Postor deberá ser partner de los productos ofertados. Deberá adjuntar carta del fabricante con referencia al proceso indicando que son partners de los productos ofertados. Se deberá indicar el nivel de partner.

IV. LUGAR DE ENTREGA DEL BIEN

Los bienes deberán ser ingresados en el Almacén AGROBANCO, ubicado en Calle Manuel Gonzáles Olaechea Nº415-419 San Isidro, Lima.

V.PLAZO DE ENTREGA DEL BIEN

El plazo de entrega es de máximo 15 días calendarios, contados a partir del día siguiente de la entrega de la orden de compra o suscripción del contrato.

VI. CONFORMIDAD DEL BIEN

Para efecto del trámite de pago, el área de Sistemas deberá otorgar la conformidad del bien dentro de un plazo de 10 días hábiles de recibido los bienes.

FORMATO N° 01

REGISTRO DEL PARTICIPANTE

NIVEL DE CONTRATACION AL QUE SE PRESENTA:

Nivel I	( )
Nivel II	( )
Nivel III	( )
Exoneración	(X)

Denominación del proceso: EXONERACION Nº 002-2017-AGROBANCO
ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB

DATOS DEL PARTICIPANTE:

(1) Nombre o Razón Social:		
(2) Domicilio Legal:		
(3) R. U. C Nº	(4) Nº Teléfono (s)	(5) Nº Fax
(6) Correo(s) Electrónico(s):		

El que suscribe, Sr.(a): _____, identificado con DNI Nº_____, representante Legal de la empresa _____, que para efecto del presente proceso de selección, solicito ser notificado al correo electrónico consignado en el cuadro precedente, comprometiéndome a mantenerlo activo durante el período que dure dicho proceso.

Lima, _____de _____ de 2017

.....
Firma, Nombres y Apellidos del postor

ANEXO N° 01

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

El que se suscribe, ……. *(o representante Legal de .....)*, identificado con DNI Nº ....., R.U.C. Nº ....., *con poder inscrito en la localidad de ..... en la Ficha Nº ..... Asiento Nº .....,* **DECLARO BAJO JURAMENTO** que la siguiente información de mi representada se sujeta a la verdad:

Nombre o Razón Social					
Domicilio Legal					
RUC		Teléfono		Fax	

Ciudad y fecha, ...

.....
Firma y sello del Representante Legal
Nombre / Razón social del postor

(*) Cuando se trate de Consorcio, esta declaración jurada será presentada por cada uno de los consorciados.

ANEXO N° 02

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL SERVICIO CONVOCADO

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

De nuestra consideración:

El que suscribe, …… (postor y/o Representante Legal de .....), identificado con DNI Nº ....., RUC Nº ..... en calidad de postor, luego de haber examinado los documentos del proceso de la referencia proporcionados por la Entidad Banco Agropecuario-Agrobanco y conocer todas las condiciones existentes, el suscrito señala que el servicio ofrecido cumple con las Especificaciones Técnicas, de conformidad con dichos documentos y de acuerdo con los Requerimientos Técnicos Mínimos y demás condiciones que se indican en el Numeral 2.3.1 de las Bases.

En ese sentido, me comprometo a la entrega del bien de conformidad con las características, en la forma y plazo especificados en las Bases.

Ciudad y fecha, ...

.....
Firma y sello del Representante Legal
Nombre / Razón social del postor

ANEXO N° 03

DECLARACIÓN JURADA

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

De nuestra consideración:

El que suscribe ……. (o representante legal de ……), identificado con DNI Nº ....., con RUC Nº ……, domiciliado en ....., que se presenta como postor de la **EXONERACION Nº 002-2017-AGROBANCO, para la ADQUISICIÓN DE RENOVACIÓN DE SOLUCION DE SEGURIDAD DE ANTIVIRUS, ANTI SPAM Y FILTRO WEB, declaro bajo juramento:**

1.- Conozco, acepto y me someto a las bases, condiciones y procedimientos del proceso de selección.

2.- Soy responsable de la veracidad de los documentos e información que presento a efectos del presente proceso de selección.

3.- Me comprometo a mantener mi oferta durante el proceso de selección y a aceptar la orden de compra, en caso de resultar favorecido con la Buena Pro.

Ciudad y fecha, ...

.....
Firma y sello del representante legal
Nombre / Razón social del postor

ANEXO Nº 04

DECLARACIÓN JURADA SOBRE PLAZO DE ENTREGA DEL BIEN

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

De nuestra consideración,

El que suscribe, don _____ identificado con D.N.I. N° _____, Representante Legal de _____, con RUC Nº _____, DECLARO BAJO JURAMENTO que mi representada se compromete a entregar el bien en el plazo de 15 días calendario, de conformidad con lo descrito en las Especificaciones Técnicas.

Ciudad y fecha, ...

.....
Firma y sello del representante legal
Nombre / Razón social del postor

ANEXO Nº 05

CARTA DE PROPUESTA ECONOMICA
(MODELO)

Señores
DEPARTAMENTO DE LOGÍSTICA
EXONERACIÓN Nº 002-2017-AGROBANCO
Presente.-

A continuación, hacemos de conocimiento que nuestra propuesta económica es la siguiente:

MONTO TOTAL S/	

El costo incluye todos los tributos, seguros, transportes, inspecciones, costos laborales, conforme a la legislación vigente, así como cualquier otro costo que pueda tener incidencia sobre el costo del bien.

Ciudad y fecha, ...

.....
Firma y sello del representante legal
Nombre / Razón social del postor

ANEXO Nº 06

CARTA DE AUTORIZACIÓN
(Para el pago con abonos en la cuenta bancaria del proveedor)

Ciudad y fecha, ...

Señor(a)
Gerente de Administración de AGROBANCO
Presente

Asunto: Autorización para el pago con abonos en cuenta

De nuestra consideración:

Por medio de la presente, comunico a Ud. que el número de cuenta de la empresa que represento es el ……(Indicar el nombre o razón social del proveedor titular de la cuenta, de ser el caso el número de CCI), agradeciéndole se sirva disponer lo conveniente para que los pagos a nombre de mi representada sean abonados en la cuenta que corresponde al Banco……

Asimismo, dejo constancia que la factura a ser emitida por mi representada, una vez cumplida o atendida la correspondiente Orden de Compra y/o de Servicio o las prestaciones en bienes y/o servicios materia del contrato quedará cancelada para todos sus efectos mediante la sola acreditación del importe de la referida factura a favor de la cuenta en la entidad bancaria a que se refiere el primer párrafo de la presente.

Atentamente,

.....
Firma y sello del representante legal
Nombre / Razón social del postor