**4.10.1 Requisitos mínimos:**

 **4.10.1.1 Oferta técnica:**

* La Carta de Presentación y Compromiso (Formulario No.1).
* Datos del oferente (Formulario No.2).
* Modelo de carta de confidencialidad (Formulario No.3).
* Ofertar todos y cada uno de los bienes y servicios ofertados.
* Soporte técnico (Formulario No.4).
* Información de accionistas de personas jurídicas (Resolución INCOP No.037-09 Formulario No. 5).
* Declaración del representante legal de la persona jurídica oferente cuyas acciones se negocian en la bolsa de valores nacionales o extranjeras (Formulario 5.2)
* Formulario de agregado nacional (Formulario No. 6 y 6A).
* Folletos y catálogos del servicio
* Copia del RUC
* Copia del RUP
* Copia de cedula del representante legal
* Datos que acrediten al representante legal (nombramiento)
* Los precios no deberán incluir el Impuesto al Valor Agregado IVA.

**ESPECIFICACIONES TECNICAS DEL SOFTWARE**

**Descripción de las Bases técnicas del producto**

El producto deberá contar con:

* Protección de Punto Final (Protección a nivel de estaciones de trabajo y servidores).
* Administración Centralizada de la solución.
* Soporte local del producto con personal calificado por el fabricante de la aplicación.

**Nota: Entiéndase por código malicioso a las siguientes clasificaciones de software**: Adware, Backdoor, Badware Alcalinos, Bombas, Bomba fork, Bots, Caballo de Troya, Cookies, Crackers, Cryptovirus, Dialers, Exploit, Hijacker, Hoaxes, Jokes, Keystroke o keyloggers, Ladilla virtual, Leapfrog, Parásito Informático, Pharming, Phishings, Pornware, Rabbit, Riskware, Rootkit, Scumware, Spam, Spyware, Ventanas emergentes/POP-UPS, Virus, Worms (gusanos).

**Característica mínima a cumplir en protección de punto final:**

* Plataformas a proteger:
* Windows 2000/XP Windows Vista/7 32 y 64bits
* Windows 8 de 32 y 64 bitsWindows Server 2000
* Windows Server 2003/2008/2012 32 y 64 bits
* Linux CentOS 5 y 6 32 y 64 bits
* El número de licencias a adquirir son 3286.
* Del total de licencias adquiridas un porcentaje igual o superior al 10% podrá ser utilizado para la instalación de servidores.

**Protección en tiempo real (motor en tiempo real).**

El producto detectará y detendrá automáticamente en tiempo real a códigos maliciosos que se quieran instalar en la PC vía e-mail, web, recursos compartidos, o dispositivos removibles (USB, sticks), para esto deberá cumplir con lo siguiente:

* El producto deberá tener motor de tiempo real capaz de detectar y detener a códigos maliciosos, en el momento de su escritura en las unidades de discos fijas o removibles (archivo nuevo) o modificación de archivo existente (infección de archivo existente).
* Deberá tener filtrado de correo electrónico realizando la búsqueda de códigos maliciosos a nivel de socket en tráfico SMTP, POP3, POP3SSL e IMAP, este debe ser independiente del cliente de correo usado, debiendo filtrar el código malicioso antes de la escritura en la base de datos del cliente de correo.
* Filtrado de SPAM en correo electrónico.
* Para el caso de la instalación en un servidor Linux con servicio de correo, el filtrado de códigos maliciosos no debe tener limitación en el número de buzones o cuentas de correo. (Indicar los servidores de correo soportados por el producto).
* Deberá incluir 3 licencias para el filtrado de códigos maliciosos en servidores de correo exim, que corren bajo servidores Linux y sin limitación en el número de buzones o cuentas de correo.
* Deberá tener filtrado de navegación realizando la búsqueda en tiempo real de códigos maliciosos en tráfico HTTP y HTTPS, debiendo filtrar el código malicioso antes de que se escriban en las carpetas temporales del disco duro.
* Deberá impedir modificaciones al sistema (cambios en el registro).
* Deberá tener la opción de realizar exclusiones de archivos del análisis en tiempo real.

**Análisis Manual (motor por demanda).**

El producto detectara los códigos maliciosos escritos en los dispositivos locales (fijos y removibles), para esto deberá cumplir con lo siguiente:

* Deberá tener la opción de correr un análisis manual de búsqueda de códigos maliciosos.
* Deberá tener la opción de realizar exclusiones de archivos del análisis del motor por demanda.
* Se deberá poder realizar análisis programados (En-Demanda) de los discos duros locales. Esta programación o agenda se puede configurar en forma diaria o semanal.

**Protección Proactiva (solo para estaciones de trabajo, no para servidores).**

La solución debe contar con protección proactiva con al menos las siguientes características:

* Cortafuegos de escritorio.- El producto deberá contar con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de trafico de Red. Contará con:
	+ Total protección para IPv4 e IPv6.
	+ Posibilidad de agregar reglas y servicios al cortafuego en forma autónoma y centralizada.
* HIPS (Host-based Intrusion Detection).- El producto contará con protección proactiva en tiempo real que contara con:
	+ IDS/IPS el cual bloqueará y registrará intentos de intrusión. Este actualizara sus plantillas de detección en forma automática desde el servidor de la solución
	+ Control de aplicaciones a la cual se le podrá agregar reglas forma autónoma y centralizada, con esta aplicación se controlará que aplicativos pueden conectarse hacia la red en forma de cliente o servidor.
* El producto deberá ser compatible con Cisco NAC.

**Características mínimas a cumplir en la administración centralizada:**

El producto contará con un servidor de la aplicación y su respectiva consola administrativa que deberá cumplir con lo siguiente:

* El servidor de la aplicación y su respectiva consola deberán instalarse sobre servidores Windows o Linux.
* La instalación de servidores de la aplicación y su respectiva consola deberán ser realizadas en un número ilimitado.
* El ingreso a la consola de administración debe ser segura y autenticarse a través de contraseña.
* Esta aplicación deberá tener la posibilidad de realizar instalaciones programadas de los productos de la solución ofertada, de igual manera la actualización de estas aplicaciones, reparación en las estaciones (herramientas desplegadas a través de consola) y remoción de la aplicación.
* Solución escalable para permitir crecimiento tanto en sitio como en localizaciones remotas con un solo servidor de la aplicación.
* Deberá poder administrar todos los módulos de protección instalados en el cliente de estación (Windows y Linux), servidores (Windows y Linux) y protección perimetral.
* Actualización a través del servidor de la solución de todas las estaciones protegidas con la posibilidad de tener redundancia de servidores de actualización en forma automáticas (Fail-over).
* La actualización de la base de datos de firmas de códigos maliciosos deberá ser incremental, ahorrando de esta manera ancho de banda en su despliegue.
* Deberá contar con un reportador gerencial detallado que de información de las configuraciones y actualizaciones de los productos, alertas, estadísticas, etc., las cuales deberán poder exportarse a archivos csv y/o html.
* Reportes gráficos tipo barra, pastel, etc., para una vista rápida de la situación del producto.
* Alerta en consola y notificación vía correo electrónico y SNMP.
* Compatibilidad con la estructura organizacional del Directorio Activo de servidores Windows para la instalación del producto.
* La administración de la consola hacia el producto de protección de punto final debe poder administrar al menos las siguientes características:
	+ Actualización de base de datos de firmas de códigos maliciosos.
	+ Bloqueo de cambio de configuración de la solución por parte del usuario.
	+ Bloqueo de la desinstalación del producto por parte del usuario aún teniendo cuenta de administrador.
	+ Bloqueo de la descarga (detener servicio) del producto por parte del usuario.
	+ Configuración del intervalo de tiempo de las consulta al servidor de la solución.
	+ Capacidad de conformar las reglas generales para todos los clientes del control de aplicaciones mediante el reporte de las estaciones de las aplicaciones que corren sobre ellas.

**Soporte local del producto con personal calificado por el fabricante de la aplicación:**

La solución deberá contar con un soporte 24x7x365 vía telefónica, correo o fax, por parte del fabricante y soporte 8x5 vía telefónica, correo o fax por parte del oferente local.

**Capacitación de la administración de la solución ofertada.**

El ofertante deberá dictar a 2 personas designadas por la ESPOL los cursos de capacitación para la administración de la solución ofertada. Los cursos deberán repetirse dos veces al año si la ESPOL lo requiere. Las personas que reciban la capacitación deberán informar al Administrador del contrato sobre este acuerdo.