

SERVICIO NACIONAL DE PATRIMONIO DEL ESTADO

SENAPE

|  |  |
| --- | --- |
|  | ESPECIFICACIONES TECNICAS  ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS Y FILTRADO DE CONTENIDOS WEB |

**FORMULARIO C-1**

**ESPECIFICACIONES TÉCNICAS**

|  |  |
| --- | --- |
| **Para ser llenado por la Entidad convocante**  **(llenar las Especificaciones Técnicas de manera previa a la publicación del DBC)** | **Para ser llenado por el proponente al momento de elaborar su propuesta** |
| **Característica Solicitada (\*)** | **Característica Propuesta (\*\*)** |
| **SOLUCION DE SEGURIDAD ANTIVIRUS** |  |
| Cantidad de licencias solicitadas: Mayor o igual a 150 licencias |  |
| Licenciamiento y servicios de un año (365 días) |  |
| Protección con modelo de distribución – SaaS Software as a Service (Software como servicio) |  |
| Infraestructura hospedada en el fabricante, Consola , Base de datos, Servidor de Administración etc. |  |
| Deberá realizar búsquedas en la red de equipos no protegidos. |  |
| Consola Web con acceso seguro por puerto HTTPS y http encriptado y comprimido, se podrá crear más de un usuario. Los usuarios creados deberán tener la opción de monitorización, administrador de seguridad y control total.  Servicio de Alojamiento (Servicio Gestionado en el fabricante), debe estar disponible 24x7x365. |  |
| La Consola Web deberá permitir la integración con herramientas de administración remota como Teamviewer, VNC, Logmein. |  |
| Deberá permitir desde la consola delegar la gestión y unificación de licencias por el proveedor de seguridad o fabricante, además de permitir organizar el control de seguridad en las máquinas en grupos, a los cuales se podrá limitar la cantidad de equipos pertenecientes, límite de instalaciones con el perfil del grupo.  Deberá permitir establecer una contraseña desde la consola web para la desinstalación del agente de comunicaciones.  Deberá permitir la administración delegando recursos de control a oficinas remotas, Divisiones o Departamentos de la Institución, sin pérdida del control centralizado en la Oficina principal o Área de Sistemas Central de la institución. |  |
| No debe requerir hardware ni software adicional. No deberá instalarse ni desplegarse ningún servicio que ocupe servicios de red o recursos en un equipo como Ej.: Internet Information Server, Crystal Reports, SQL Server, MySQL y Microsoft Management Console). |  |
| Debe contar con las siguientes protecciones mínimas:  Anti-spyware, Anti-rootkit, Anti-phishing, Detección Proactiva (Heurístico) antimalware, Protección E-mail, Protección para mensajería instantánea, Protección para robo de identidad, Protección para MS Exchange.  Filtro Antispam para trafico entrante y saliente, además de análisis de los buzones de mail y de transporte. |  |
| Firewall Personal gestionado, que cuente con: Filtrado de aplicaciones; Filtro de acceso a redes (por direcciones, puertos y protocolos); Prevención que cuente con un detector y bloqueador de intrusiones IDS; Prevención de virus de red con detección y bloqueo de intentos de exploits realizados mediante técnicas de desbordamiento de buffer y Configuraciones basadas en Zonas (red de Confianza y red Pública) que pueda ser administrada de manera centralizada o desde el cliente. |  |
| Filtro de Navegación HTTP/HTTPS, filtrado de navegación por perfiles y por al menos 50 categorías sin la necesidad de instalar complementos o plugins en los navegadores web. |  |
| Deberá contar con una tecnología que analice los archivos trasmitidos por mensajería instantánea IM antes que accedan al PC. |  |
| Deberá contar con una tecnología que analice los archivos adjuntos en correo SMTP, POP3 y MAPI antes que accedan al PC. |  |
| Deberá contar con sistema de control de dispositivos (Device Control) en el mismo cliente. Que permita las siguientes configuraciones a los dispositivos:  -USB, HDD - Bloquear , permitir lectura, Permitir lectura y escritura  -CD/DVD - Bloquear, permitir lectura, Permitir lectura y escritura.  - BLUETOOTH – Bloquear, Desbloquear.  - DISPOSITIVOS DE IMAGENES como Cámaras web, scanners o similares.- Bloquear, Desbloquear  . MODEMS, se refiere a módems USB 3G , usados como métodos de navegación con operadores por redes de operadores como ENTEL, TIGO y VIVA o similares. – Bloquear, Desbloquear |  |
| Debe contar con Herramienta de Distribución propio del fabricante. |  |
| Deberá ser compatible para instalación por MSI compatible con herramientas de distribución estándar como Tivoli, login scripts, LanDesk, etc. |  |
| Deberá contar con Instalación vía e-mail automático para los usuarios externos a la LAN con URL de instalación. |  |
| Updates y Upgrades de motor y ficheros de firmas mediante vía web de bajo de consumo de ancho de banda o mediante sistema P2P entre clientes los cuales deben ser programables. En caso que un equipo no disponga de acceso a Internet, el producto deberá contar con una tecnología Proxy, que permita que las actualizaciones y comunicaciones necesarias se realicen a través de otro equipo que si disponga de conexión a Internet, para ello el producto ofertado deberá contar con mecanismo de configuración tipo Proxy Estático desde la consola web para dirigir las peticiones de actualizaciones. |  |
| Interfaz para usuario con funciones de análisis rápidos y análisis completos al sistema. |  |
| Actualizaciones locales y bajo demanda |  |
| Sistemas operativos soportados para estaciones de trabajo (obligatorio): |  |
| Windows XP (32 y 64 bits) |  |
| Windows Vista (32 y 64 bits) |  |
| Windows 7 (32 y 64 bits) |  |
| Windows 8 y 8.1 (32 y 64 bits) |  |
| Sistemas operativos soportados para Servidores (obligatorio): |  |
| Windows Server 2003 (32 y 64 bits) |  |
| Windows Server 2008 (32 y 64 bits) |  |
| Windows Server 2012 (32 y 64 bits) |  |
| Sistemas de correo soportados (obligatorio): |  |
| Microsoft Exchange 2003 |  |
| Microsoft Exchange 2010 |  |
| Microsoft Exchange 2013 |  |
| Sistemas operativos soportados adicionales (no obligatorio, pero se considerará): |  |
| Android 2.2 y superior |  |
| Ubuntu 12 (32 y 64 bits) |  |
| Red Hat Enterprise Linux 6.0 64 bits |  |
| Debian Squeeze |  |
| OpenSuse 12 32/64 bits |  |
| Suse Enterprise Server 11SP2 64 bits  Protección de correo ZIMBRA |  |
| Compatible con Motores de Virtualización (no obligatorio, pero se considerará): |  |
| VMWare ESXi 5,x |  |
| VMWare Workstation 6.0, 6.5, 7.x, 8.x y 9.x |  |
| Virtual PC 6.x |  |
| Microsoft Hyper-V Server 2008 R2 y 2012 3.0 |  |
| Citrix XenDesktop 5.x, XenClient 4.x, XenServer y XenApp 5.x y 6.x |  |
| Deberá contar con Cuarentena corporativa |  |
| La solución deberá ofrecer informes configurables sobre malware detectado, los cuales podrán ser exportables a formatos de archivo compatibles (Ms Excel, texto plano csv, etc) |  |
| Los informes Ejecutivos deberán ser configurables en formatos periódicos (días o mes) |  |
| La solución deberá ofrecer informes Programables de Estado, Ejecutivos resumidos, y de detección por perfiles o por el total |  |
| Debe contar con Servicios de Actualizaciones Automáticas diarias con un factor de aplicación de configuraciones en un tiempo menor o igual a los 15 minutos |  |
| Debe contar con Servicios de Actualizaciones manuales con un factor de aplicación de configuraciones en un tiempo menor a los 3 minutos |  |
| Debe contar con Servicios de Actualizaciones express ante epidemias de virus u otro tipo de malware |  |
| Debe contar con Servicios de Alertas sobre virus. |  |
| La solución deberá permitir cambio de versiones y tipo de producto de acuerdo a las características técnicas del parque informático y las características dinámicas de la red, o segmentos de red de la institución. Particularmente en las situaciones técnicas que por limitaciones de performance de PCs no se pueda acceder a tecnología de protección gestionada, garantizando de igual manera la protección total de estos segmentos o grupos de PCs. |  |
| Certificaciones y detalles de los centros de datos del fabricante |  |
| Al tratarse de una solución SaaS el proveedor deberá contar con las certificaciones mininas de la industria y seguridad para el manejo de información: |  |
| ISO27000 |  |
| ISO/IEC 27001:2005 |  |
| Statement on Auditing Standards No. 70 (SAS 70) Type I and II |  |
| Sarbanes-Oxley (SOX) |  |
| PCI DSS |  |
| Federal Information Security Management Act (FISMA) |  |
| El producto ofertado deberá contar con certificaciones Checkmark , West Coast y otras de la industria de la seguridad de información y tecnología antimalware. |  |
| El fabricante deberá ser en lo posible miembro de la AMTSO - Anti-Malware Testing Standards Organization (opcional, pero se considerará). |  |
| El proponente deberá presentar Certificado de Distribución y Comercialización Autorizado para Bolivia emitido por el fabricante (En caso de que el Software ofrecido sea de origen extranjero). La certificación también debe señalar, que la antigüedad como distribuidor y comercializador de soluciones de software de seguridad informática del fabricante, para Bolivia, sea mínima de cinco años. (Demostrable, presentar curriculum de la empresa en fotocopia simple). |  |
| El proponente deberá contar, mínimamente con Dos técnicos certificados por el fabricante en el producto ofertado, para proporcionar soporte técnico, presentar curriculum en fotocopia simple |  |
| Se debe capacitar al personal de la Institución, en curso técnico de instalación y administración del producto, Describir si la empresa proporciona otras formas de capacitación |  |
| La empresa ofertante deberá contar con al menos 2 (Dos) años de experiencia en la comercialización autorizada del producto |  |
| En la oferta se deberá incluir los siguientes servicios: |  |
| Soporte técnico y apertura de casos por gestión de CRM directamente desde el fabricante. (Obligatorio) |  |
| Soporte Técnico 24/365 vía e-mail |  |
| Soporte Técnico Web |  |
| Soporte Técnico telefónico o “in situ” en horarios de oficina |  |
| Actualizaciones a nuevas versiones |  |
| Actualizaciones de sus firmas de detección cada hora. |  |
| **REQUISITOS DE LAS ESPECIFICACIONES TÉCNICAS** |  |
| **SOFTWARE DE SEGURIDAD PARA FILTRADO DE CONTENIDOS** Firewall, IPS, VPN, Antimalware, Content Filter, Antispam, Web Filter, QoS, Hotspot. |  |
| Soporte de usuarios: Mayor o igual a 100 usuarios |  |
| El software deberá contar con actualizaciones desde el fabricante. |  |
| Consola Perimetral de Administración Se deberá tener acceso a una consola segura utilizando protocolo  HTTPS para ver el estado de todos los segmentos de red configurados y poder ser administrados. |  |
| Administración y Configuración Interfaz web seguro (HTTPS) intuitivo a través de cualquier navegador. Acceso remoto configurable. |  |
| Esta gestión deberá ser del mismo fabricante bajo acceso seguro HTTPS con una credencia de acceso para el administrador. |  |
| Administración desde la nube para monitorizar estado de la solución, actualización de forma centralizada desde cualquier lugar y cualquier momento. |  |
| Modo de funcionamiento en capa 2 y 3 Modo Router NAT Modo Bridge/Transparente |  |
| Soporte para múltiples tecnologías de conexión WAN ADSL/UMTS/GPRS/3G/WIRELESS |  |
| Actualizaciones Tipo: Automático sin necesidad de intervención por parte del usuario. |  |
| Restauración y actualización de sistema de manera local o remota |  |
| Respaldo (Backup) de configuración exportable por tarea programada y capaz de ser enviado de forma periódica por email a la cuenta del administrador |  |
| Respaldo (Backup) podrá ser importado local y de forma remota. |  |
| Protocolos que debe analizar mínimamente.  HTTP, HTTPS, FTP, SMTP, POP3 para Contenidos TCP, UDP e ICMP para intrusiones de las red mediante IPS SSL. IPSEC y L2TP para Redes privadas Virtuales |  |
| POLITICAS DE SEGURIDAD Se deberá permitir la creación de políticas de acceso para todo tipo de tráfico. |  |
| FIREWALL Rendimiento Firewall: mayor o igual a 620 Mbps Compatible velocidades 10/100/1000 Política basada en NAT. IPS con reglas de más de 5000 Ataques y actualizables de forma automática |  |
| FILTRADO DE APLICACIONES  Filtrado de aplicaciones por puerto en uso, como Facebook, Twitter, Youtube, Whatsapp, Box, DropBox, Tor, o similares.  Deberá poder bloquear el acceso por puertos HTTP y HTTPS. |  |
| PROXY Se deberá incluir funcionalidad de Proxy incluyendo el modo transparente para agilizar el acceso a las páginas más visitadas. |  |
| ALTA DISPONIBILIDAD Deberá ser capaz de aceptar por lo menos dos conexiones a Internet de manera redundante o paralela y que permita la administración de ancho de banda. |  |
| Redes Privadas  VPN Protocolos SSL, IPSec, PPTP y L2TP. Métodos de Cifrado: DES, 3DES, AES, BlowFish, TwoFish y Serpent Soporte Gateway-Gateway, Gateway-Roadwarrior Túneles Dedicados: Ilimitados |  |
| CALIDAD DE SERVICIO Se deberá contar con QoS configurable para dar prioridad al trafico vital y prioritario |  |
| DHCP para asignación de direcciones IP de forma automática y en reserva, la cual deberá incluir un listado de Acceso autorizados por MAC |  |
| DNS Dinámico |  |
| POLITICAS DE ADMINISTRACION |  |
| ·          Definir y editar políticas de seguridad, incluyendo horarios. |  |
| ·          Definir objetos y grupos de objetos |  |
| ·          Definir redes y grupos de redes. |  |
| ·          Definir servicios y grupos de servicios. |  |
| ·          Definir usuarios y grupos de usuarios. |  |
| ·          Gestionar actualizaciones y copias de seguridad. |  |
| ·          Configuración del servicio de registros de eventos del firewall. |  |
| ·          Definir servicios (http, dns, ident, etc.) |  |
| ·          Definir interfaces de red y reglas de ruteo. |  |
| ·          Creación de reglas de traducción de red (NAT) |  |
| ·          Configurar conexiones VPN. |  |
| ·          Configurar la detección de escaneo de puertos. |  |
| ·          Definir reglas de calidad de servicio (QoS) para la gestión efectiva del ancho de banda. |  |
| ·          Definir reglas de filtrado de paquetes. |  |
| Motor antimalware deberá ser del mismo fabricante, no deberá ser de un tercero. |  |
| CONTENT FILTER: Filtrado de contenidos en protocolos de transporte HTTP y FTP, Protocolos de correo y Noticias SMTP, POP3 como mínimo. |  |
| ANTISPAM - Filtrados de Spam - Filtrado de Spam para protocolos de mensajería - Capacidad de eliminar/redirigir en tiempo real - Uso de firmas digitales para correos sospechosos - Consultas a servidores externos para detección de spam - Acciones para spam y probable spam - Listas Blancas y negras de Dominios, IPs y Direcciones. - Análisis de trafico entrante y saliente |  |
| FILTRADO WEB , P2P/IM - Filtrados Web y P2P/IM - Filtrado por 50 categorías o más - Filtrado en tiempo real - Actualización de bases de datos |  |
| HOTSPOT Acceso a redes Wifi bajo control en segmento seguro, el cual podrá ser configurado por el administrador. La configuración del Hotspot deberá permitir al administrador dar acceso limitado a los recursos Wifi de la red bajo las condiciones de: Tiempo Cantidad de Sesiones Ticket para autenticación |  |
| PRECIO REFERENCIAL DE TODA LA SOLUCIÓN  48,122.00Bs. Cuarenta y ocho mil ciento veintidós 00/100 Bolivianos. |  |

***Nota.-*** *Las personas naturales y/o Empresas nacionales, deberán presentar sus propuestas, hasta horas 16:00 del día jueves 18 de junio de 2015, En la avenida Hugo Estrada N° 94, zona Miraflores, edificio del SENAPE, 1er. piso, oficina de Adquisiciones, la apertura de sobres se realizará el mismo día a horas 16:05.*

*La Paz, junio de 2015*