SERVICIO NACIONAL DE PATRIMONIO DEL ESTADO

SENAPE

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS Y FILTRADO DE CONTENIDOS WEB

FORMULARIO C-1

ESPECIFICACIONES TÉCNICAS

ANTIVIRUS CORPORATIVO

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 (**)**
REQUISITOS DE LAS ESPECIFICACIONES TÉCNICAS	
SOLUCION DE SEGURIDAD CORPORATIVO Antimalware , Firewall, Antispam, Filtrado Web HTTP/HTTPS, Control de Dispositivos.	
Periodo de contrato: Servicios por un año calendario (365 días)	
Cantidad de Licencias:185 licencias Antivirus	
CARACTERISTICAS DEL PRODUCTO SOLICITADO	
Infraestructura hospedada en el fabricante, Consola Administrativa, Base de datos.	
Deberá realizar búsquedas en la red de equipos no protegidos.	
Consola Web con acceso seguro por puerto SSL, se podrá crear más de un usuario. Los usuarios creados deberán tener la opción de monitorización, administrador de seguridad y control total	
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	
El acceso a la consola deberá ser de forma segura vía https y http encriptado y comprimido.	
Seguridad como servicio, 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, CrystalReports, SQL Server, MySQL y Microsoft Management Console).	
Anti-spyware	
Anti-rootkit	

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
Anti-phishing	
Detección Proactiva (Heurístico) antimalware	
Protección E-mail	
Protección para mensajería instantánea	
Protección para robo de identidad	
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.	
Monitorización de la Navegación HTTP/HTTPS, si el administrador desea la solución deberá monitorizar la navegación para futuras acciones correctivas.	
Filtro de Navegación HTTP/HTTPS, filtrado de navegación por perfiles y por categorías.	
El filtrado deberá estar integrado con el mismo cliente de Protección Antivirus el cual deberá filtrar la navegación de cualquier navegador sin la necesidad de instalar complementos o plugins en estos.	
Filtrado de navegación HTTP/HTTPS podrá ser configurado por horas en grupos y subgrupos como defina el administrador.	
Filtrado de navegación HTTP/HTTPS podrá ser configurado por horas en grupos y subgrupos como defina el administrador.	
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.	

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
Control de dispositivos (Device Control). Esta tecnología ofrece una protección adicional ante la entrada de malware a través dispositivos externos a la vez que permite aumentar la productividad evitando el uso ineficiente de los mismos. Esta tecnología deberá ser desarrollada por el mismo fabricante, deberá estar incluida en el cliente de protección permitiendo el control de : USB, HDD - Bloquear , permitir lectura, Permitir lectura y escritura CD/DVD - Bloquear , permitir lectura, Permitir lectura y escritura BLUETOOTH – Bloquear DISPOSITIVOS DE IMAGENES – Bloquear MODEMS – Bloquear * Dispositivos de imágenes como Cámaras web, scanners o similares. *Modems se refiere a modems USB, usados como métodos de navegación con operadores por redes de operadores como ENTEL, TIGO y VIVA o similares.	
Protección avanzada para Blindaje de sistemas, de ataques del tipo Ransomware (Encriptadores). Generación de logs y grafos de la actividad del malware Esta protección deberá evitar que el ramsonware encripte información en las PCs (CryptoLocker)	
Herramienta de Distribución (opcional)	
Deberá instalar por MSI compatible con herramientas de distribución estándar como Tivoli, SMS, login scripts, LanDesk, etc.	
Instalación vía e-mail automático a los usuarios con URL de instalación	
Updates y Upgrades vía Web con consumo mínimo de ancho de banda.	
Actualizaciones de motor y ficheros de firmas programables por el administrador, para definir que días y a que hora se realizaran estos procesos.	
Consola local para usuario final.	
Interfaz para usuario con análisis rápidos y completos al sistema.	

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
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.	
Deberá poderse configurar un Proxy Estático desde la consola web para dirigir las peticiones de actualizaciones	
Tecnología P2P, que permita detectar si los ficheros de instalación o actualización se encuentran disponibles en otro equipo de la red para así obtenerlos de ese equipo y no desde internet.	
Actualizaciones locales y bajo demanda	
Sistemas operativos soportados para estaciones de trabajo: Windows XP, Windows Vista, Windows 7, Windows 8 y 8.1, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 enversiones de 32 y 64 bits	
Sistemas de correo : Microsoft Exchange 2003 o superior, Android 2.2 y superiores Ubuntu 12 (32 y 64 bits) o superior, Red Hat Enterprise Linux 6.0 64 bitso superior.	
Compatible con Motores de Virtualización VMWare ESX 3.x,4.x, 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	
Deberá contar con Consola Web para el administrador, permitiendo configurar las protecciones de manera remota por grupos y perfiles de protección.	
Deberá contar con Consola Web para Administrador, permitiendo gestionar y monitorizar las protecciones y las detecciones (malware y sospechosos)	
Deberá contar con Cuarentena corporativa	
La Consola Web para cliente deberá 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.	
La consola deberá permitir la creación de Grupos y subgrupos para de estaciones y servidores para mayor control y generación de políticas por grupo o subgrupo.	

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
Deberá permitir establecer una contraseña desde la consola web para la desinstalación del agente de comunicaciones.	
Deberá permitir establecer una contraseña desde la consola web para la desinstalación de la protección local.	
Deberá lograr Gestión de la seguridad por perfiles y grupos	
Deberá permitir la configuración de actualizaciones (up grades) desde la consola Web	
Deberá permitir la administración delegando recursos de control a oficinas remotas de la Institución, sin pérdida del control centralizado en la Oficina Central SENAPE.	
La solución deberá ofrecer informes configurables sobre malware detectado, los cuales podrán ser exportables a formatos compatibles, txt, xls, csv como mínimo.	
Los informes Ejecutivos deberán ser configurables en formatos periódicos (días o mes).	
La solución deberá ofrecer informes sobre procesos de actualización.	
La solución deberá ofrecer informes Programables de Estado, Ejecutivos resumidos, y de detección por perfil o por el total	
Servicio de Alojamiento (Servicio Gestionado en el fabricante),debe estar disponible 24*7 y contar con un servicio de gestión que monitorice constantemente el estado de los servicios y aplicaciones tomando acción en caso de incidencias y de esa manera garantizar que el servicio de filtrado esté siempre disponible.	
Debe contar con Servicios de Actualizaciones diarias	
Debe contar con Servicios de Actualizaciones express ante epidemias de virus u otro tipo de malware	
Debe contar con Servicios de Alertas sobre virus.	
Debe contar con Servicios de Actualizaciones del software automáticas, tanto de las protecciones como de las mejoras en la consola de administración	
El fabricante deberá ser en lo posible miembro de la AMTSO - Anti-Malware TestingStandardsOrganization	
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	

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**
El proponente deberá contar, mínimamente con Dos técnicos certificados por el fabricante en el producto ofertado, para proporcionar soporte técnico. (adjuntar en la propuesta C.V. de los técnicos en fotocopia simple, en caso que se requiera se solicitará los ORIGINALES)	
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	
2 (Dos) años como mínimo de experiencia en la comercialización autorizada del producto.(Demostrable)	
Servicios incluidos de:	
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.	
LUGAR DONDE SE PRESTAN SERVICIOS DE ASISTENCIA TÉCNICA: En caso de detectarse problemas con el software del contrato, el servicio de asistencia técnica deberá ser llevado a cabo en las dependencias del Servicio Nacional de Patrimonio del Estado	
ENTREGA E INSTALACIÓN: La entrega e instalación del Software debe realizarse en oficinas del Servicio Nacional de Patrimonio del Estado, sin que ello implique un costo adicional	
PLAZO DE ENTREGA La licencias o Certificado electrónico del Software debe ser entregado en formato impreso máximo en 5 días calendario, después de firmado el contrato.	
VALIDEZ DE LA COTIZACIÓN No menor a 25 días calendario	
PRECIO REFERENCIAL Bs.21,700.00Veinte y un mil setecientos 00/100 Bolivianos	

FORMULARIO C-1

SISTEMA DE FILTRADO DE CONTENIDOS Y REDES VPN

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 (**)**
REQUISITOS DE LAS ESPECIFICACIONES TÉCNICAS	
SOFTWARE PARA ADMINISTRACION DE GATEWAY DE FILTRADO DE CONTENIDO y APLICACIÓNES. Firewall, IPS, VPN, Antimalware, Filtrado de contenido, Antispam, Filtrado por aplicación, QoS, Hotspot.	
Deberá ser compatible con la infraestructura en uso de la institución.	
La solución ofertada NO deberá ser ensamblada y/o contener software no empresarial. Incluir Documentación de respaldo que avale este punto.	
El software de la solución deberá contar con actualizaciones desde el fabricante.	
La solución ofertada deberá tener acceso a la"Consola de Administracióny Configuración" segura, intuitiva a través de cualquier navegador Web utilizando protocolo seguro HTTPS.	
La solución ofertada deberá contar con configuración de Acceso remoto por HTTPS para ver el estado de la solución propuesta desde un único punto.	
Administración desde la nube para monitorizar estado, cambio de configuraciones y/o actualización de forma centralizada desde cualquier lugar y cualquier momento.	
Modo de funcionamiento en capa 2 y 3 Modo Router NAT Modo Bridge/Transparente.	
La solución ofertada deberá tener la capacidad de administrar 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.	
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.	
Protocolos analizados 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	

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**
POLITICAS DE SEGURIDAD Se deberá permitir la creación de políticas de acceso para todo tipo de trafico	
FIREWALL Rendimiento Firewall: 620 Mbps mínimamente Compatible velocidades 10/100/1000mbps Política basada en NAT. IPS con reglas de más de 5000 Ataques y actualizables de forma automática.	
FILTRADO DE APLICACIONES Filtrado de aplicaciones 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 Backup de líneas y alta disponibilidad para el acceso a internet, con soporte para tecnología USB 3G/UMTS/GRPS. Deberá ser capaz de aceptar por lo menos dos conexiones a Internet de manera redundante o paralela, aplicando sobre ellas mecanismos de priorización de paquetes y división de ancho de banda por usuarios, grupos, rango de ips o segmentos de redes. (Administración de ancho de banda)	
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	
La solución ofertada deberá contar con manejo de 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.)	

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
· 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.	
MALWARE: Análisis HTTP de al menos 180 Mbps, SMTP 388.000 Mensajes por día mínimamente. Protocolos analizados: HTTP, HTTPS, FTP, SMTP, POP3 como mínimo. Detección de Virus, Gusanos, Troyanos, Dialers, Jokes, Herramientas de hackeo, Spyware, Phishing.	
Motor antimalware deberá ser del mismo fabricante.	
FILTRADO DE CONTENIDOS: Filtrado de contenidos en protocolos de transporte HTTP, HTTPS y FTP, Protocolos de correo y Noticias SMTP, POP3.	
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 categorías: mínimamente 60 categorías - Filtrado en tiempo real: Si - Actualización de bases de datos : Si - Reportes exportables: En formato compatibles xls, txt, o csv	
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	
LUGAR DONDE SE PRESTAN SERVICIOS DE ASISTENCIA TÉCNICA: En caso de detectarse problemas con el software del contrato, el servicio de asistencia técnica deberá ser llevado a cabo en las dependencias del Servicio Nacional de Patrimonio del Estado	

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**
ENTREGA E INSTALACIÓN: La entrega e instalación del Software debe realizarse en oficinas del Servicio Nacional de Patrimonio del Estado, sin que ello implique un costo adicional	
PLAZO DE ENTREGA La licencias o Certificado electrónico del Software debe ser entregado en formato impreso máximo en 5 días calendario, después de firmado el contrato.	
VALIDEZ DE LA COTIZACIÓN No menor a 25 días calendario	
PRECIO REFERENCIAL Bs.18,800.00Diez y ocho mil ochocientos 00/100 Bolivianos	

Nota.- *Las personas naturales y/o jurídicas, deberán presentar sus propuestas, hasta horas 16:00 del día jueves 22 de junio de 2017, 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 2017