ADENDA Nº 01

CONTRATACION Directa para la "Adquisición de Software"

PAC Nº 39/11

A LOS OFERENTES PARTICIPANTES DE LA CONTRATACION DIRECTA PARA LA ADQUISICION DE SOFTWARE, EN LO REFERENTE A:

ANEXO 1

Instrucciones para los oferentes y datos del procedimiento de Contratación Directa.

El Oferente podrá presentar con su oferta los siguientes documentos adicionales;

a) Nombre del BANCO y el número de Cuenta Corriente a nombre de la empresa, en el que se acredite el pago y deberá estar avalada por una certificación del BANCO, en original o copia autenticada, conforme el Decreto Nº 7781/06.
b) Fotocopia simple de la cédula de identidad del firmante de la oferta;
c) Fotocopia simple de la cédula tributaria del oferente (RUC);
d) Certificado De Cumplimiento Tributario vigente;
e) Fotocopia simple de: Patente Comercial;
f) Fotocopia del Balance General de los últimos (2) dos años de funcionamiento (2009, 2010).
g) Declaración Jurada por la cual se garantiza que ni el oferente ni sus proveedores se encuentran involucrados en prácticas que violen los derechos de los menores estipulados en la Constitución Nacional, los Convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el Código del Trabajo, el Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la Republica del Paraguay.
h) Copia del Anexo "3" firmado y/o documentos que acrediten que el bien cumple con las especificaciones técnicas (catálogos; planillas de datos; declaraciones; certificados; etc.)
i) Estatuto Social vigente y sus modificaciones (si las tuviere), para el caso de las Sociedades.

PARA EL ITEM 1. Servidor Antivirus Corporativo (*): se deberá acreditar, lo siguiente:

j) El oferente debe poseer certificación de la marca o del representante mayorista para la comercialización del producto. **Se deberá presentar la correspondiente certificación.**
k) El oferente debe poseer por lo menos 2 (dos) años de experiencia en el mercado con productos de la marca. **Se deberá presentar copia de contratos de los últimos dos (2) años, referente al servicio solicitado en el presente llamado.**
l) El oferente debe poseer por lo menos un técnico certificado por la marca para la implementación del producto. **Se deberá presentar certificación de la marca para el técnico que estará a cargo de los trabajos en la CGR**
m) El oferente debe poseer un técnico con experiencia en la solución corporativa de Mcafee para el proceso de desinstalación del mismo. **Se deberá presentar currículo del técnico que estará a cargo de los mencionados trabajos en la CGR.**

PARA EL ITEM 5. VMware vCenter Server 4 Foundation for vSphere up to 3 hosts. Basic Support / Subscription for vCenter Server 4 Foundation for vSphere y SNS is Required Technical Support, 12 Hours/Day, per published Business Hours, Mon. thru fri

Requisitos que se debe cumplir para la instalación:

n) El oferente debe poseer certificación de la marca o del representante mayorista para la comercialización del producto. **Se deberá presentar la correspondiente certificación.**

o) El oferente debe poseer por lo menos tres (3) años de experiencia en el mercado con productos de la marca. **Se deberá presentar copia de contratos de los últimos tres (3) años, referente al servicio solicitado en el presente llamado.**

p) El oferente debe poseer por lo menos dos (2) técnicos certificados por la marca para la implementación del producto. **Se deberá presentar certificación de la marca para el técnico que estará a cargo de los trabajos en la CGR**

La Contraloría General se reserva el derecho de verificar in situ las instalaciones de los oferentes.

SE ACLARA QUE LOS DOCUMENTOS SOLICITADOS EN EL PUNTO 11. SON INDISPENSABLES PARA LA EVALUACION DE LA CAPACIDAD TECNICA, ECONOMICA Y FINANCIERA DEL OFERENTE, POR LO EN CASO DE NO PRESENTARSE CON LA OFERTA, LA CGR SOLICITARA LA PRESENTACION DE LOS MISMOS DENTRO DEL PLAZO DE 24 HORAS. DE NO PRESENTARSE DICHOS DOCUMENTOS EN EL PLAZO ESTABLECIDO, LA OFERTA SERA DESCALIFICADA.

ANEXO 2

Formulário de carta/oferta. Procedimiento de Contratación Directa N° 39/2011 "Adquisición de Software". ID N° 215043.

Ítem	Código Catálogo	Descripción	Marca del Producto	Procedencia	Unidad de Medida	Presentación	Cantidad	Precio Unitario(IVA incluido)
1	43233205-002	Servidor Antivirus Corporativo (*)			Unidad	unidad	400	
2	43233205-006	WebFilter 500 seats 18 Months Renew - SKU WS-J-CP18-R - Estas licencias tendrán vigencia a partir de diciembre			Unidad	unidad	500	
3	43233205-006	WebFilter 500 seats 6 Months Renew - SKU WS-J-CP06-S			Unidad	unidad	250	
4	43232901-001	Basic Support Coverage VMware vSphere 4 Standard for 1 processor (Max 6 cores per processor)			Unidad	unidad	4	
5	43232901-001	VMware vCenter Server 4 Foundation for vSphere up to 3 hosts. Basic Support / Subscription for vCenter Server 4 Foundation for vSphere SNS is Required Technical Support, 12 Hours/Day, per published Business Hours, Mon. thru Fri Debe incluir la instalación y configuración del software para gestionar dos servidores disponibles.			Unidad	unidad	1	
							Precio Total (IVA Incluido)	

ANEXO 3

"Adquisición de Software". ID Nº 215043.

Cantidad, descripción y especificaciones técnicas mínimas de los servicios requeridos.

Ítem	Código Catálogo	Descripción	Unidad de Medida	Presentación
1	43233205-002	Servidor Antivirus Corporativo (*)	Unidad	unidad
2	43233205-006	WebFilter 500 seats 18 Months Renew - SKU WS-J-CP18-R - Estas licencias tendrán vigencia a partir de diciembre	Unidad	unidad
3	43233205-006	WebFilter 500 seats 6 Months Renew - SKU WS-J-CP06-S	Unidad	unidad
4	43232901-001	Basic Support Coverage VMware vSphere 4 Standard for 1 processor (Max 6 cores per processor)	Unidad	unidad
5	43232901-001	VMware vCenter Server 4 Foundation for vSphere up to 3 hosts. Basic Support / Subscription for vCenter Server 4 Foundation for vSphere SNS is Required Technical Support, 12 Hours/Day, per published Business Hours, Mon. thru Fri Debe incluir la instalación y configuración del software para gestionar dos servidores disponibles.	Unidad	unidad

(*) ESPECIFICACIONES TÉCNICAS DEL SERVIDOR ANTIVIRUS CORPORATIVO

1. CONSOLA DE ADMINISTRACION

Características	Especificación técnica requerida
A) Requerimientos de Operación:	
1. La consola deberá proporcionar una "interfaz gráfica" para la administración, configuración y operación del Sistema.	SI
2. Poseer un mecanismo de identificación de usuarios para el acceso a la consola de administración el cual se integre a Active Directory.	SI
3. El almacenamiento de las claves de acceso deberá realizarse en forma encriptada con algoritmos de robustez reconocida internacionalmente.	SI
4. La aplicación deberá conectarse a la base de datos con una cuenta que posea los menores privilegios.	SI
5. Limitar la cantidad de conexiones simultáneas a la base de datos, ya sea por medio de un control a través de la base de datos o por medio del aplicativo.	SI
6. La aplicación no deberá requerir privilegios de Administrador Local para su ejecución en los nodos de la red.	SI
7. El control de acceso y los derechos de uso y operación serán definidos mediante perfiles propios de la aplicación. Los usuarios estarán asociados a estos perfiles, de manera tal de heredar todos los derechos asociados.	SI
8. El sistema deberá permitir definir de manera flexible a que transacciones, funcionalidades o atribuciones podrán acceder los distintos niveles o perfiles de usuarios. Estos perfiles deberán definirse de forma tal que se respete la separación de funciones y así lograr un adecuado control por oposición.	SI
9. Cierre de Sesión: El sistema inhabilitará la operación en el puesto de trabajo y requerirá una nueva autenticación a cualquier usuario que no registre actividad por un período de 15 (quince) minutos.	SI
B) Registros de Seguridad y reportes de auditoria.	
1. El sistema debe permitir registrar y emitir todas las actividades operativas de los usuarios (log transaccional), las tareas realizadas y las funciones utilizadas. Dicho registro deberá contener como mínimo: fecha y hora, ID del usuario, transacción realizada, perfil del usuario, su ubicación en la red, resultado de la operación (Exitosa o Fallida) y detalle de la operación realizada o información adicional.	SI
2. Deberán existir reportes de seguridad que registren la asignación de derechos de accesos, actividades de los usuarios privilegiados y accesos especiales. Estos reportes deben poder ser visualizados e impresos en forma ordenada, o filtrados por cualquiera de los datos que componen los mismos.	SI
3. Deberán existir reportes de auditoría que registren las excepciones y actividades criticas de las distintas plataformas.	SI

Características	Especificación técnica requerida
4. El sistema deberá permitir realizar la exportación de los archivos de registros de seguridad y reportes de auditoría para su análisis off-line y su almacenamiento.	SI

2. PROTECCIÓN DE NODOS DE RED

Características	Especificación técnica requerida
1. Se requiere la provisión de una solución para la protección de los nodos de red que incluya Antivirus, Firewall, IPS, y control de dispositivos USB,	SI, Especificar
2. La solución deberá estar licenciada para la totalidad de **400 nodos** de red.	SI
3. La solución deberá permitir incluir las actualizaciones de firmas, versiones y updates de Virus por el periodo solicitado	**12 meses**
4. Administrar de manera centralizada y realizar tareas de instalación, actualización y configuración remota de los nodos protegidos por la solución.	SI
5. Visualizar globalmente, de manera resumida y en tiempo real, el estado de los nodos protegidos por la solución.	SI
6. Administrar la configuración de los distintos componentes de la solución permitiendo configurar los distintos programas de la solución en tiempo real.	SI
7. Administrar la configuración de los distintos componentes de la solución permitiendo configurar los distintos programas de la solución sin depender de una agrupación en dominios.	SI
8. Deberá efectuar la instalación de todos los componentes de la solución de forma automática sin intervención del usuario en forma flexible. Ejemplo: Login script, ejecutable, vía remota.	SI
9. La herramienta de protección no deberá requerir aplicaciones adicionales para comunicarse a la consola de administración. Es decir con un único agente que se ejecute la herramienta cubrirá los aspectos de seguridad y comunicación con la consola.	SI
10. Deberá poder desinstalar el antivirus actual de la máquina en forma automática (si se encuentra el ejecutable de desinstalación del antivirus dentro del nodo de red).	SI
11. Iniciar rastreos parciales o totales en los nodos protegidos de la red.	SI
12. Planificar rastreos automáticos especificando nodos protegidos de la red.	SI
13. Organizar los nodos protegidos de la red en grupos.	SI
14. Efectuar tareas de monitoreo de los nodos protegidos.	SI
15. Restringir parcial y totalmente el acceso de los usuarios finales a la configuración local de los productos de protección instalados.	SI
16. Limitar a los usuarios para que no puedan desinstalar ni bajar de memoria la protección antivirus de la solución.	SI
17. El sistema deberá contar con la posibilidad de instalar los agentes en forma remota.	SI
18. Obtener las actualizaciones de listas de virus y motores de búsqueda en forma automática y programada desde el sitio de Internet del proveedor.	SI
19. Obtener las actualizaciones de mejoras y nuevas versiones desde el sitio de Internet del proveedor.	SI
20. Configurar el modelo de obtención de actualizaciones por Push o Pull o ambas.	SI
21. Permitir incorporar las actualizaciones de manera manual, por medio magnético y desde el sitio de Internet del proveedor o fabricante de la solución.	SI
22. Distribuir las actualizaciones de manera incremental, automática y desatendida.	SI
23. Distribuir actualizaciones sin tener que realizar nuevas validaciones, ni depender de la agrupación de los equipos informáticos en dominios.	SI
24. Utilizar servidores secundarios en modalidad cascada para efectuar las distribuciones de actualizaciones en forma automática.	SI
25. Posibilidad de Configurar en los agentes una cadena de actualización. Ejemplo: Si el servidor 1 no esta disponible comprobar en el servidor 2	SI
26. La solución deberá contar con control de dispositivo USB, PCMCIA, CD/DVD, Serial, Firewire y Bluetooth con las siguientes características:	SI
26.1 Bloquear el acceso a los dispositivos no autorizados.	SI
26.2 Aplicar políticas por tipo dispositivo y que este integrado a la estructura de usuarios del Directorio Activo de windows.	SI
27. La solución deberá incluir módulo de IPS HOST en el agente con las siguientes funcionalidades:	SI

27.1 Bloquear las conexiones cuando se detecta un ataque hacia un recurso compartido desde una computadora infectada.	
27.2 Capacidad de definir programas confiables.	SI
27.3 Capacidad para detectar programas no deseados y de tomar acciones para cuando haya una detección.	SI
27.4 Deberá permitir la creación de políticas restrictivas para evitar la transferencia de datos de una placa Ethernet a una placa Wifi (bloqueando la placa Wifi)	SI
28. Las configuraciones de los puntos 26, 27 al 28 se podrán aplicar por: Máquina, grupo y Usuario del Directorio Activo para el caso de control de dispositivos.	SI
29. La solución deberá permitir las siguientes funcionalidades respecto a los Reportes y Notificaciones al detectar un virus:	-
29.1 Generar reportes centralizados estadísticos y gráficos de toda la solución.	SI
29.2 Emitir notificaciones de los incidentes de virus en los nodos protegidos.	SI
29.3 Emitir las notificaciones a los administradores con alguno de los siguientes métodos: • Correo electrónico • Generación de alarma sonora o visual en puestos de trabajo • Registro de evento en syslog (local y remoto) • Registro de evento en eventlog • Trap SNMP.	SI, Especificar
29.4 Configurar el contenido y los destinatarios de las notificaciones.	SI
29.5 Visualizar las notificaciones en la consola de administración.	SI
29.6 Generar reportes de los nodos protegidos.	SI
29.7 Los reportes deberán contener la siguiente información de las nodos protegidos de la red: • Dirección IP. • Sistema operativo y versión. • Configuración del producto de protección instalado en el nodo. • Versión del Motor de Rastreo y Lista de Virus. • Estado de la conexión con el servidor. • Listado de archivos con virus. • Resumen del último escaneo realizado.	SI
30. No requerir el reinicio de la estación de trabajo protegida luego de la actualización de listas de virus y motores de búsqueda.	SI
31. Realizar escaneos en tiempo real.	SI
32. Iniciar escaneos por demanda del usuario, de manera programada y por demanda del Administrador de manera remota.	SI
33. Detectar Spyware, Virus Troyanos, malware y demás virus existentes.	SI
34. Detectar los virus en archivos compactados del tipo: cab, zip, tar, arj, etc.	SI
35. Detectar virus en archivos compactados y anidados con un mínimo de 5 niveles.	SI
36. Reparar archivos que contengan macros infectadas.	SI
37. Eliminar archivos que contengan virus de script.	SI
38. Eliminar componentes ActiveX maliciosos.	SI
39. Configurar las acciones a tomar ante la detección de un virus.	SI
40. La solución deberá permitir las siguientes funcionalidades respecto a las acciones y procedimientos a seguir ante la detección de virus: Contemplar las siguientes acciones a tomar ante la detección de virus en archivos: • Reparar el archivo infectado. • Eliminar el archivo infectado. • Mover el archivo infectado a una carpeta particular de cuarentena. • Reportar el incidente. En caso que no sea posible ejecutar la acción, el sistema deberá contar con la posibilidad de ofrecer una segunda opción a tomar.	SI

3. INFRAESTRUCTURA

Características	Especificación técnica requerida
1. El sistema en su modalidad de Antivirus debe poder ejecutarse en los nodos de red con las siguientes plataformas: • MS Windows 2000 Workstation • MS Windows 2000 Server • MS Windows 2000 Advanced Server • MS Windows XP Professional • MS Windows 2003 Server • MS Windows 2003 Advanced Server • MS Windows 7 (32 y 64 bits) • MS Windows 2008 Standard (32 y 64 bits) • MS Windows 2008 Enterprise • Linux • Vmware	SI
2. Características técnicas y funcionalidades respecto a la protección de servidores de correo electrónico:	-
2.1. Proteger de virus informáticos los mensajes de correo electrónico.	SI
2.2. Instalarse sobre MS Exchange 2003 o superior brindando todas las funcionalidades requeridas en protección de servidores de correo electrónico en el presente pliego.	SI
2.3. Efectuar rastreos de virus con las diferentes APIs de detección de virus de Microsoft en MS Exchange: MAPI, AVAPI, VSAPI.	SI
2.4. Contar con integración a bajo nivel con MS Exchange interactuando con el "Information Store", protegiendo la integridad de los mensajes, adjuntos y las bases de datos respectivamente.	SI
2.5. No deberán existir restricciones en cuanto a la cantidad de cuentas a administrar y proteger que afecten el correcto funcionamiento de la solución.	SI
2.6. Configurar acciones en tiempo real y de manera programada.	SI
2.7. Deberá permitir rastreo de virus en los archivos adjuntos sobre los mensajes en tiempo real	SI
2.8. Deberá permitir las siguientes acciones sobre los mensajes de manera programada: • Realizar rastreos de virus sobre MailBoxes de usuarios. • Programar rastreos. • Realizar rastreos incrementales. • Permitir reportar, desinfectar, eliminar, mover el archivo infectado adjunto al correo electrónico.	SI
2.9. Configurar las acciones a tomar ante la detección de un virus.	SI
2.10. Reportar incidentes de detección de virus.	SI
2.11. Enviar notificaciones al administrador y al emisor y al receptor del mensaje.	SI
2.12. Configurar los destinatarios de las notificaciones permitiendo deshabilitar al emisor o al receptor del mensaje.	SI
2.13. Configurar el texto de la notificación que se entregará al receptor y al emisor del mensaje.	SI

4. PROTECCIÓN DE CORREO ELECTRÓNICO ANTIVIRUS Y ANTISPAM

Características	Especificación técnica requerida
1. Se requiere la provisión basada en appliance virtual en entorno vmware para la protección de correo electrónico que incluya Antivirus, Antispam y Filtro de contenido	SI, Especificar
2. Deberá proveerse una solución tipo Appliance específico de alta performance con capacidades de escalabilidad y con funcionalidades integradas de seguridad	SI, Especificar
3. La solución deberá estar licenciada para la totalidad de **usuarios 400**	SI, Especificar
4. Mediante el soporte de las diversas metodologías de la solución, debe proporcionar un nivel de detección de al menos: 99 %	SI
5. Mecanismo de control para la limitación de la tasa de tráfico por alguno de los siguientes métodos: • Dirección IP del remitente. • Reputación IP del remitente. • Período de tiempo.	SI, Especificar
6. Funcionalidad de MTA	-
6.1 El appliance deberá poder actuar como Gateway para el tráfico SMTP entrante y saliente	SI
6.2 Reporte de errores cuando se excede la cantidad de conexiones permitidas por el appliance	SI
6.3 Control de conexiones simultáneas para correos entrantes	SI
6.4 Soporte para múltiples colas de correo	SI

6.5 Manejo de Protocolos de correo SMTP y ESMPT	SI
6.6 Soporte SMTP sobre TLS	SI
6.7 TLS configurable por dominio	SI
6.8 DNS Internal resolver/cache; Posibilidad de resolución utilizando DNS local o Servidores Root de Internet	SI
6.9 Deberá soportar reverse DNS	SI
6.10 Integración LDAP con Active Directory.	SI
6.11 Deberá contar con sistemas de protección ante ataques de denegación de servicio, ataques de Directorio (Harvest Directory) y día cero	SI
6.12 Bloqueo de correo con identidades forjadas (spoofing) ya conocidas	SI
6.13 Debe permitir bloquear mensajes originados externamente, pero que dicen ser de un dominio interno (Domain Spoofing Detection)	SI
6.14 Bloquear ataques de rebote (bounce attacks)	SI
6.15 Debe poder comprobar la validez del remitente mediante alguna de las siguientes tecnologías: reverse DNS, Bounced Address Tag Validation (BATV), Address Lookup.	SI, Especificar
6.16 Monitoreo en tiempo real del flujo de correos obteniendo información detallada por Dominio y dirección IP.	SI
7. Funcionalidad de Filtrado de correo	SI
7.1 Filtrado para el tráfico SMTP entrante y saliente	SI
7.2 Bloqueo o limitación de cantidad de conexiones ante un remitente no válido basado en la información de:	-
7.2.1 IP origen	SI
7.2.2 Rango de IP´s	SI
7.2.3 Dominio	SI
7.2.4 DNS	SI
7.2.5 Reputación IP.	SI
7.3 Reconocimiento de fuentes conocidas de spam y bloquearlas a nivel de conexión.	SI
7.4 Verificación de que los correos entrantes fueron enviados desde sistemas de correo confiables.	SI
7.5 Protección contra el correo no deseado, no solicitado e inadecuado incluyendo mecanismos que permitan validar la reputación del remitente, el análisis heurístico, el filtrado de URL insertadas y la detección de correo incorrecto	SI
7.6 Filtros por firmas	SI
7.7 Manejo de reglas de bloqueos personalizadas (listas blancas, negras)	SI
7.8 Listas de aceptación para servidores de correo, servidores de retransmisión, usuarios de correo electrónico y dominios de confianza.	SI
7.9 Manejo de reglas por grupos de destinatarios	SI
7.10 Opción de filtrado por "Null senders".	SI
7.11 Se debe incluir un Filtro de Reputación a través de una base de datos propietaria por Sender IP y dominio	SI
7.12 Prevención de correo no deseado utilizando como base proveedores de listas RBL.	SI
7.13 Comprobación agresiva en el encabezado de los mensajes.	SI
7.14 Filtrado de mails con encabezados malformados	SI
7.15 Prevención de correo no deseado utilizando como base búsquedas de cadenas de expresiones regulares en el contenido, encabezado y archivos adjuntos de los mensajes.	SI
7.16 Prevención de correo no deseado basada en una lista de denegación interna para servidores de correo, servidores de retransmisión, usuarios de correo electrónico y dominios.	SI
7.17 Prevención de correo no deseado utilizando como base un diccionario predefinido de correo no deseado.	SI
7.18 Detección de correo obsceno	SI
7.19 Reconocimiento del tipo de archivo adjunto utilizando como base su real tipo de extensión o contenido.	SI
7.20 Identificación del tamaño de archivos adjuntos con configuración de los valores mayor que, menor que, entre o exacto.	SI
7.21 Detección de archivos adjuntos por tipo de MIME	SI
7.22 Identificación del nombre de archivo adjunto.	SI
7.23 Exploración de palabras clave del archivo adjunto para MS Word y Adobe PDF.	SI
7.24 Detección de mensaje parcial.	SI
7.25 Detección de mensaje encriptado PGP y S\Mime.	SI
7.26 Adición de mensajes de extensión de responsabilidad.	SI
7.27 Prevención de DOS para archivos adjuntos comprimidos y mensajes anidados.	SI
7.28 Detección y prevención de asuntos o archivos adjuntos de gran tamaño.	SI
7.29 Detección y prevención de correo no deseado utilizando como base LDAP para evitar la aceptación de mensajes de correo entrante dirigidos a destinatarios no válidos y limitar el número de destinatarios no válidos en destinatarios no válidos y limitar el número de destinatarios no válidos en una misma sesión de SMTP.	SI

7.30 Examinar enlaces de correo electrónico incrustados.	SI
7.31 Aplicación de políticas antispam y de filtrado de correo por LDAP/AD o por creación de grupos locales.	SI
7.32 Poder realizar backups y restore de las configuraciones	SI
8. Funcionalidad de antivirus	-
8.1 Escaneo de virus integrado en el appliance virtual de correo electrónico entrante y saliente	SI
8.2 Motor de exploración antivirus de máxima potencia con capacidad para desinfectar y eliminar archivos adjuntos infectados.	SI
8.3 Actualización de firmas de antivirus en forma automática y manual vía protocolos HTTP, HTTPS o FTP.	SI
8.4 Las actualizaciones de las firmas de Virus deberán realizarse como mínimo diariamente o inmediatamente después de un comunicado de la firma nueva.	SI
8.5 Asegurar la integridad de las actualizaciones de definición de virus.	SI
8.6 El antivirus debe ser capaz de detectar virus, worms y otros malware basado en un análisis de contenido por firmas y heurístico.	SI
8.7 Protección proactiva: deberá brindar protección contra las amenazas conocidas y desconocidas como también contra una variedad de ataques de código activo, como aquéllos basados en Java, ActiveX y VBScript, que pueden ejecutarse automáticamente al visitar ciertos sitios Web o al utilizar el correo electrónico.	SI
8.8 Configuración de alertas y acciones automáticas.	SI
8.9 Escaneo del contenido de archivos adjuntos y comprimidos.	SI
8.10 Puesta en cuarentena de mensajes de correo.	SI
8.11 Soporte para remover adjuntos infectados y poner en cuarentena mensajes infectados.	SI
8.12 Cuando un archivo adjunto es removido, el usuario recibirá el cuerpo del correo sin el adjunto informando dentro del dicho correo las razones por las que se removió el adjunto.	SI
8.13 Envío de mensajes personalizables al usuario cuando posea correos en cuarentena.	SI
9. Consola de Administración	SI
9.1 Proveer una consola de administración Centralizada, que permita supervisar todas las amenazas de contenido.	SI
9.2 Soporte de conexión para administración bajo protocolos SSH o SCP.	SI
9.3 Registro de actividades y contenido del correo electrónico.	SI
9.4 Estadísticas de tráfico.	SI
9.5 Estadísticas de spam, virus.	SI
9.6 Estadísticas de rendimiento del servidor.	SI
9.7 Estadísticas de utilización del servidor.	SI
9.8 Enviar alertas para eventos críticos relacionados con hardware o software del producto.	SI
9.9 Debe poder configurarse enviar traps SNMP para el envio de alertas.	SI
9.10 Proporcionar una completa información histórica para el mensaje que está siendo buscado.	SI
9.11 Visualización de las colas de mensaje.	SI
9.12 Proveer estadisticas en tiempo real sobre:	-
9.12.1 Remitentes inválidos	SI
9.12.2 Correos filtrados por reputación	SI
9.12.3 Correos filtrados por spam	SI
9.12.4 Correos filtrados por detección de virus	SI
9.12.5 Correos filtrados por mensajes saneados	SI
9.12.6 La información debe estar disponible por dominio y por dirección IP	SI
9.13 Poder realizar backups y restore de las configuraciones	SI
9.14 La solución debe poder integrar una ayuda en la administración	SI
10. Cuarentena	SI
10.1 Cuarentena auto administrada por el usuario en tiempo real.	SI
10.2 Soporte para remover adjuntos infectados y poner en cuarentena mensajes infectados.	SI
10.3 Proveer al usuario la posibilidad de liberar, poner en lista blanca o borrar el mensaje.	SI
10.4 Los usuarios podrán revisar sus mails spam y eventualmente moverlos a sus casillas de inbox.	SI
10.5 Los mensajes a los usuarios para avisos de correo en cuarentena podrán ser configurables.	SI
10.6 Los correos de aviso al usuario de correo en cuarentena deberán contener un link o similar para la liberación del estado de cuarentena.	SI
11. Reportes	-
11.1 Debe permitir reportes históricos de estadísticas de uso y spam	SI
11.2 Debe permitir obtener reportes bajo demanda o programados en formatos HTML, texto o CSV.	SI
11.3 Monitoreo del flujo de correo entrante y saliente en términos de hora, día, semana y mes.	SI

11.4 Los reportes programados podrán ser enviados vía mail.	SI
11.5 Poder customizar el envío de reportes a determinados recipientes por un periodo de tiempo.	SI
11.6 Proveer estadísticas de mail y Throughput	SI
11.7 Reportes de todos los mensajes o por grupo del dominio	SI
11.8 Reporte de volúmenes de correo por usuario (destinatarios/remitentes con virus, spam, volumen y tamaño de mail)	SI
11.9 Reporte de volúmenes por dominio (volúmenes por dominio de correos con virus y spam)	SI
11.10 Creación de reportes personalizados	SI
11.11 Reportes por violación de políticas o filtro de contenidos	SI
11.12 Reportes por epidemias de virus	SI
11.13 Reportes de virus entrantes y salientes	SI

INSTALACION E IMPLEMENTACIÓN DEL ANTIVIRUS CORPORATIVO

Debe incluir la instalación y configuración del software en un servidor en entorno virtualizado con la plataforma VMware.

Actualmente se dispone de la solución corporativa de Mcafee; para la implementación de la solución, se deberá instalar el nuevo antivirus en otro servidor y en un proceso planificado ir desinstalando los nodos clientes con el Mcafee e instalar el nuevo antivirus hasta completar la totalidad de los nodos.

Así mismo, la solución antivirus y antispam se instalará inicialmente sobre un servidor Exchange, igualmente, el oferente deberá realizar la desinstalación de la solución de Mcafee e implementar la solución del nuevo antivirus y antispam.

Una vez verificado la desinstalación completa de los nodos, se deberá deshabilitar la solución de Mcafee.

En una segunda etapa, la Contraloría General se encuentra en un proceso de migración del servidor de correo electrónico Exchange a una solución sobre Linux, para este caso, el oferente se **comprometerá por escrito** a realizar el cambio de la configuración del antivirus y antispam sobre la plataforma Exchange al nuevo servidor sobre Linux, utilizando la funcionalidad de análisis por Gateway para el tráfico SMTP entrante y saliente de la nueva solución antivirus y antispam.

PLAZO DE ENTREGA DE OFERTAS: hasta las 10:00 hs., del día **20/07/11**.

FECHA DE APERTURA DE SOBRES: A las 10:30 hs., del día **20/07/11**.

FECHA TOPE DE CONSULTAS: hasta las 09:00 hs. del día **12/07/11**.

SE MANTIENEN INALTERABLES LAS DEMAS CONDICIONES INDICADAS EN LA INVITACION.

Asunción, 05 de julio de 2011.

ARQ. LILIAN GONZALEZ.
Dirección de Administración y Logística
Titular UOC
Contraloría General de la República