

Resumen

Este documento es una especificación técnica para la adquisición de software (antivirus y Windows), licencias, hardware, servicios de soporte, administración y capacitación. Los items podrán ser adjudicados de forma independiente.

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

1. Objeto del llamado

La Dirección General de Registros llama a cotización para adquirir:

Item A: antivirus corporativo y protección de dispositivos

1. **Licencias de software antivirus** según especificaciones en el presente documento
2. **Configuración** según especificaciones en el presente documento
3. **Capacitación** sobre los paquetes de software, según especificaciones en el presente documento
4. **Protección de dispositivos de los puestos de trabajo**, según especificaciones en el presente documento

Los servidores estarán localizados en las oficinas centrales (18 de Julio 1730) y los clientes, unos 600 PC's, estarán distribuidos, teniendo un 70% en las oficinas centrales y el resto en 20 sucursales en todo el país.

Item B: licencias de Microsoft Windows

1. **Software y licencias** hasta los indicados y según especificaciones en el presente documento

Item C: configuración de dominio Windows

1. **Instalación del software** según especificaciones en el presente documento
1. **Transferencia de conocimiento al personal de DGR** según especificaciones en el presente documento

Los servidores estarán localizados en las oficinas centrales (18 de Julio 1730) y los clientes, unos 600 PC's, estarán distribuidos, teniendo un 70% en las oficinas centrales y el resto en 20 sucursales en todo el país.

Item D: capacitación Windows

1. Capacitación de Microsoft Windows, según especificaciones en el presente documento

Item E: servidores

1. **2 Servidores** para controladores de dominio Windows, según especificaciones en el presente documento

2. Item A: antivirus corporativo

2.1. Características del software antivirus

- El producto debe poseer una arquitectura que contemple una consola de gerenciamiento (HTTP, HTTPS), servidores de gerenciamiento y clientes.
- Utilizar los protocolos HTTP y/o HTTPS para comunicación a la consola de gerenciamiento.
- Poseer mecanismo de comunicación en tiempo real entre servidores y clientes, que permitan la entrega de archivos de configuración y vacunas.
- Poseer un mecanismo de comunicación entre los clientes y los servidores, cuya periodicidad deberá poder ser determinada por el administrador, para consulta de nuevas configuraciones y vacunas.

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- Se valorará la capacidad de agregar nuevas características y futuras funcionalidades vía plug-ins en forma flexible y controlada.
- Instalación remota de las estaciones de trabajo.
- Protección contra desinstalación y desactivación no autorizada del producto.
- Instalación y actualización del software sin intervención del usuario.
- Descubrir las estaciones de trabajo de la red que no posean el cliente de antivirus instalado.
- El Software debe poder instalarse en equipos con sistemas operativos Microsoft Windows Server 2008, Windows XP y Vista.
- Compatible para instalaciones en servidores con S.O. Microsoft Windows Server 2008.
- Compatible con máquinas con arquitectura de 32-bits y 64-bits.
- Gestión / administración remota a través de una consola de administración centralizada única, la cual debe poder accederse por HTTP o HTTPS.
- La consola de gestión debe mostrar en tiempo real la lista de servidores y estaciones que tienen el antivirus instalado, conteniendo la siguiente información mínima: nombre de la máquina, versión de antivirus, versión del motor, fecha de la vacuna, la última fecha de verificación y el estado. Es deseable que muestre el usuario que está conectado en la estación de trabajo.
- La consola de gestión debe permitir establecer los permisos de manera que sólo el administrador pueda cambiar la configuración, desinstalar o detener el antivirus de las estaciones.
- Posibilidad de rollback de la última versión anterior de vacunas, desde la consola de administración.
- Posibilidad de agrupar estaciones de trabajo, para poder aplicar una configuración específica para cada grupo.
- Administración centralizada de la consola de gestión con un mínimo de configuración, instalación del cliente, los registros e informes.
- Capacidad de aplicar diferentes reglas basadas en la lógica de la red. Por ejemplo: distintas horas de actualización de los agentes según grupos predefinidos, o distintas reglas de firewall, de scaneo, etc.
- Opción de exportar los informes en formato HTML y/o PDF.
- Protección en tiempo real contra virus, gusanos, caballos de troya, spyware, adware y otros tipos de código malicioso.
- Detección y eliminación de virus de macro, en tiempo real.
- Se valorará positivamente la verificación de virus en mensajes de correo electrónico, dentro de la estación de trabajo. Adjuntar lista de clientes de correo soportados.
- El Anti-spyware de protección debe poder administrarse con la consola central ya solicitada.
- La configuración de anti-spyware debe hacerse a través de la misma consola de virus.
- Auto-reparación de los daños causados por virus, como los del tipo "caballo de Troya". Dicha reparación automática no deberá requerir personal o paquetes adicionales. Esta función debe ser nativa de la solución, por lo que deberá actualizarse de forma automática y sin necesidad de intervención por parte del administrador.
- Posibilidad de realizar escaneos de forma manual y programada en las estaciones de trabajo.
- Posibilidad de colocar archivos y directorios en las listas de exclusiones de la verificación del virus
- Protección contra virus de red, siendo la gestión de forma centralizada.

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- La verificación de virus y reparación de archivos "infectados" dentro de archivos comprimidos en por lo menos los siguientes tipos: ZIP, RAR, ARJ y CAB.
- Se valorará que posea la capacidad de, en caso de epidemia, bloquear el acceso a las carpetas compartidas, el TCP y UDP, y el acceso para escribir y borrar archivos y directorios específicos, y luego el restablecimiento de la configuración original al final de la epidemia.
- Se valorará que permita la reanudación de los servicios de antivirus de forma automática en el caso de que algún virus o código malicioso haya detenido los mismos, sin necesidad de intervención por el administrador.
- Se valorará que permita configurar prioridades de CPU para realizar el escaneo tanto agendado como automático.
- Permitir establecer medidas que deben adoptarse con la aparición de virus, incluyendo: reparación, eliminación, mover a la cuarentena y pasar por alto.
- Se valorará que posea la capacidad de remover automáticamente el total de los daños causados por el spyware, adware y gusanos, tales como la limpieza de registro y los puntos de carga, con una opción para finalizar el proceso y poner fin al servicio de la amenaza en el momento de su detección.
- La remoción automática de los daños causados deberá ser nativo del anti-virus, que no depende de plugin, o módulo adicional.
- Se valorará la posibilidad de ejecutar remotamente el escaneo de virus con la posibilidad de seleccionar una máquina o grupo de máquinas para el escaneo.
- Permitir que el escaneo de las amenazas tanto de manera manual, programada o en tiempo real, detecten amenazas en el nivel Kernel del sistema operativo proporcionando la posibilidad de detección de rootkits.
- Capacidad para detectar keyloggers por el comportamiento de los procesos en memoria con una variedad de diferentes sensibilidades de detección.
- Capacidad para detectar troyanos y gusanos por el comportamiento de los procesos en memoria, con la opción de la sensibilidad de las distintas detecciones.
- La configuración del firewall personal deberá realizarse a través de la misma consola de administración de antivirus.
- Se valorará la posibilidad de agendar la activación de reglas (escaneo, reglas del firewall para determinado horario, etc.).
- Posibilidad de crear reglas para diferentes aplicaciones.
- Poseer protección contra exploración de buffer overflow.
- Poseer protección contra ataques de Denial of Service (DoS), Port-Scan, MAC Spoofing y IP Spoofing.
- Se valorará la posibilidad de ofrecer bloqueo de conexiones a URLs e IP's maliciosas que una máquina pueda hacer. No sólo para el navegador, sino para toda conexión HTTP que la máquina puede hacer. Se valorará también la posibilidad de ofrecer distintas capacidades de políticas para diferentes máquinas.
- Notificación automática al administrador en caso de una epidemia de virus.
- Almacenamiento de logs en caso de ocurrencia de virus en el registro local y en el log del servidor remoto.
- Proporcionar las notificaciones en caso de cualquier anomalía en la red (IDS, firewall personal y virus de red).

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- Generación de alerta en caso de los virus, a través de mensajes en la pantalla, SNMP y correo electrónico (SMTP).
- Poseer alertas y registros gráficos en la propia consola de administración.
- Actualización incremental automática de las vacunas y la versión del software en los servidores. Las horas de actualización deberían ser configurables. La actualización debería permitir la conexión a través de un proxy.
- El suministro de vacunas para nuevos virus será suministrado en un plazo máximo de 24 horas.
- Actualización incremental de los clientes, a distancia y en tiempo real, sin la necesidad de utilizar login-scripts, sin intervención por parte del usuario, y sin necesidad de reiniciar la máquina para su aplicación. Todo esto deberá funcionar sin necesidad de módulos adicionales que no sean parte de la solución.
- Proporcionar un solo archivo que incluya la vacuna para todas las plataformas Windows y las versiones del virus.
- Se valorará que permita crear planes para la distribución de actualizaciones.
- Se valorará la posibilidad de elegir cualquier cliente administrado a los efectos de que oficie de servidor para la distribución de actualizaciones dentro de una sub-red. Éste cliente haría las descargas incrementales del servidor y las distribuiría para los demás clientes de su sub-red.
- Actualización remota e incremental del software de los clientes.
- Se valorará la posibilidad de aplicar políticas de bloqueo preventivo de una amenaza para el período en que la vacuna aún no esté disponible a los efectos de detener la propagación. Ejemplos de estas políticas: bloqueo de los puertos a los que se extiende la amenaza, bloquear el nombre del archivo infectado, proteger un directorio particular, bloquear la red para un conjunto de máquinas.
- Se valorará que tenga un mecanismo de copia de seguridad y restauración de la base de datos de la solución, en la consola de gestión integrada. En caso de no tenerlo, el proveedor deberá indicar el procedimiento de respaldo.
- Debe disponer de las últimas certificaciones ICSA Labs por lo menos en los sistemas operativos Windows XP, Windows Vista y Windows Server.

2.2. Opcional: protección de dispositivos de los puestos de trabajo

Este punto es opcional y puede no ser adjudicado junto con los otros puntos del ítem. Asimismo, sólo podrá ser adjudicado junto con el resto de los puntos del ítem, por lo que no es considerado un ítem en sí mismo.

Se busca una solución de software que permita controlar la conexión de dispositivos a los PC's.

Características:

- Consola de administración centralizada. La administración de la solución de protección de dispositivos debe estar integrada a la consola de administración del antivirus.
- Administrador Local no puede remover aplicación
- Driver a nivel de Kernel
- Administración vía Web
- El agente debe permanecer activo cuando el equipo está desconectado de la red
- Mensaje de alerta frente a mal funcionamiento
- Monitoreo y comunicación de eventos en tiempo real
- Aplicación de políticas por máquina, usuario, grupo y tipo de dispositivo.

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- Deberá ser capaz de controlar las siguientes interfaces:
 - USB
 - PCMCIA
 - FireWire
 - LTP
 - Bluetooth
 - IrDA
 - Wifi
 - Disk Drives
 - Human Interface Devices
 - IDE ATA/ATAPI controllers
 - IEEE1284.4 compatible printers
 - IEEE1284.4 devices
 - IEEE1394 IP Network Emulator
 - INFINIBAND
 - Keyboards
 - Medium Changes
 - Mice and other pointer device
 - Adaptadores Multifuncionales
 - Network Adapter
 - Network client
 - Plug & Play and Non-Plug & Play Drivers
 - Other Devices (customized)
 - SBP2 IEEE 1394 Devices
 - SCSI and RAID Controllers
 - Security acelerators
 - Smart Cards Readers
 - Storage volume shadow copies
 - Impresoras de red
 - Windows CE USB
- Deberá ser capaz de interactuar con los siguientes Dispositivos:
 - Almacenamiento Masivo (en modalidad Permitido/Bloqueo/Solo Lectura)
 - Disquete
 - Disco Duro externo
 - Unidades de cinta
 - Memorias

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- Modem
- Impresoras de Red
- Grabador de CD
- Smartphone
- Palm
- Sería deseable que se pudieran agregar otros dispositivos personalizados
- Deberá poder funcionar sobre plataformas Windows XP/Vista
- Aplicación en tiempo real de políticas
- Notificaciones configurables
- Reporta qué dispositivo está actualmente conectado en el PC
- Suspensión remota de políticas
- Sincronización con Active Directory
- Instalación Remota
- Desinstalación Remota
- Reporte de los agentes conectados en tiempo real
- Actualización automática
- Modulo de reportes vía Web
- Exportación de reportes a otros formatos (CSV, etc.)

2.3. Configuración

El proveedor deberá instalar el software en al menos 2 servidores Windows y 20 PC's de la sede de Montevideo.

2.4. Capacitación

Se capacitarán hasta 5 funcionarios de la División Informática. Se deberá especificar el temario. En caso de corresponder, cotizar distintos niveles y cantidades de alumnos.

3. Item B: licencias de Microsoft Windows

Se requiere las siguientes licencias de Microsoft Windows:

Part Number	Item Name	Cantidades
P72-01102	Windows Svr Ent Lic/SA Pack OLP NL GOVT	2
R18-01634	Windows Server CAL Lic/SA Pack OLP NL GOVT Device CAL	600

4. Item C: configuración de dominio Windows

Se deberá instalar dos servidores Windows Enterprise Server 2008 con los siguientes servicios:

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

- Ambos serán controladores de dominio
- File server
- WSUS
- Configuración de políticas. Esto debe incluir, pero no limitarse a, los siguientes elementos: políticas de passwords, deshabilitar para ciertos usuarios o grupos el autorun y los dispositivos USB en los PC's, configurar el Resultant Set of Policy (RSOP) snap-in, auditorías de distintos eventos en el servidor (e.g. acceso de los usuarios a recursos del servidor). Se valorará la presentación de una propuesta de configuración de políticas que incluya los elementos antes mencionados, más los que el proveedor entienda convenientes para agregar valor a su propuesta.
- También se deberá configurar 20 PC's con Windows XP o Vista de manera que queden funcionando como parte del dominio y las políticas configuradas en el servidor se apliquen correctamente en estos PC's.
- Cotizar el costo de configuración de 100 PC's. DGR podrá contratar opcionalmente en caso necesitarlo la configuración de PC's en cantidades que sean múltiplos de esa cifra.
- El proveedor, luego de instalar y configurar los servidores, deberá dedicar al menos 20 hs a la transferencia tecnológica de la instalación realizada. Dicha transferencia tecnológica deberá realizarse luego de que el personal de la Dirección General de Registros haya finalizado la capacitación, a fin de que puedan aprovechar mejor esta transferencia.
- Cotizar el costo de la administración de los servicios anteriores mencionados por un período de 1 año, extensible hasta 3 años.

6. Item E: servidores

6.1. 2 Servidores para dominio Windows

Se necesita adquirir 2 servidores compatibles con Windows Enterprise Server 2008.

La configuración mínima de cada servidor debe ser la siguiente:

- Tipo rack mount, para racks de 19" (incluir kit de montaje)
- Lectora/grabadora de DVD
- Ventiladores y fuentes de poder redundantes
- 2 procesadores Quad Core Intel® Xeon® X5460, 2x6MB Cache, 3.16GHz, 1333MHz FSB
- 16GB de RAM de 667 MHz (4x4GB)
- 3 x 300GB SAS 15K RPM Internos, con capacidad de agregar por lo menos un disco más.
- Controladora Interna de RAID
- 2 Placas de red GigaEthernet

7. Folletos

1. Los oferentes deberán entregar conjuntamente con la oferta, información técnica amplia y detallada de los elementos cotizados, incluyendo folletos originales redactados en idioma español o inglés, ilustraciones, etc., que permitan apreciar ampliamente el material ofrecido. En el caso del **software**, considerando que mucha veces éste se vende simplemente entregando los números de las licencias, la folletería podrá ser sustituida por material descargado de la web.
2. La División Informática de la Dirección General de Registros podrá solicitar posteriormente

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

información complementaria y/o muestras del material cotizado en caso de ser necesario.

8. Garantía de calidad

1. Deberá cotizarse un servicio de soporte técnico de referencia y emergencia, con respuesta en menos de 24 horas. Se valorará la posibilidad de reportar directamente al fabricante en aquellos casos en que la División Informática de la Dirección General de Registros lo entienda conveniente.
2. Deberá especificarse claramente qué empresa brindará el servicio técnico referido y con qué recursos cuenta, lo cual podrá ser tenido en cuenta al momento de adjudicar.
3. El proveedor deberá establecer la garantía por escrito en su oferta. Ella deberá ser fácilmente comprensible y legible, y deberá informar a la División Informática de la Dirección General de Registros sobre el alcance de sus aspectos más significativos.

9. Condiciones y requisitos particulares

1. La empresa deberá tener experiencia probada en la instalación de la solución ofertada, en la Administración Pública o en empresas de gran porte. Deberán brindarse referencias de ello, en un número no inferior a tres.
2. La empresa deberá disponer de técnicos capacitados en las herramientas ofrecidas. Se deberá incluir, junto a la oferta, la nómina de personal que se encargaría de este proyecto, así como el curriculum vitae de cada uno de ellos, y el tiempo de permanencia en la empresa.

10. Condiciones y requisitos generales

1. Los items podrán ser adjudicados de forma separada a diferentes proveedores.
2. La División Informática de la Dirección General de Registros podrá solicitar la instalación del software ofertado para realizar las pruebas que se crean pertinentes. A dichos efectos, el mismo deberá ser instalado en sus oficinas (18 de Julio 1730, 4º piso) cuando ésta lo disponga, permaneciendo en ellas un mínimo de 30 días hábiles desde su instalación.
3. Todo el software entregado deberá estar acompañado de las licencias de uso correspondientes, o aclarar específicamente si es gratuito.
4. Todas las características mencionadas corresponden a especificaciones mínimas para que el producto ofertado sea tenido en cuenta, pero en ningún caso deberán considerarse como límite superior de las características de los equipos a ofertar.
5. La solución debe ser total, completa, y deben abarcar todos los componentes, electrónica, eléctrica, red, kits, y demás insumos y mano de obra para su puesta en producción. Todo elemento no detallado en este pliego y necesario para la puesta en producción de la solución global, la empresa oferente deberá detallarlo, cotizarlo e incluirlo en la propuesta económica. De no ser así se asume incluido en sus costos.
6. La garantía y mantenimiento técnico debe ser total y por un período mínimo de 3 años, especificando los costos anuales.
7. Se priorizarán certificaciones brindadas por fabricantes a la empresa sobre productos, las cuales serán tomada como nivel de especialización y capacidad de servicio, frente a otras ofertas que no los tuvieran.

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha:

Item quitado:

5. Item D: capacitación Windows

Se deberá incluir cursos oficiales dictados en un Centro Autorizado de Instrucción.

Cotizar el costo por persona.

Incluir los siguientes cursos:

- Administración de estaciones de trabajo y servidores
 - Windows Server 2008 Network Infrastructure
 - Windows Server 2008 Active Directory
- Managing and Maintaining Windows Server 2008 Servers

Redactado: Marcos Orfila	Revisado: Gerardo Ferrari	Aprobado:
Fecha: 15/05/2009	Fecha:	Fecha: