CONTRATACIÓN DIRECTA N° 11/2018 – ID N° 349.350
"ADQUISICIÓN DE SERVIDORES"

ADENDA N° 02

La Sub Unidad Operativa de Contrataciones del Consejo de la Magistratura – Escuela Judicial, procede a realizar la siguiente Adenda:

MODIFICACIÓN DE LAS ESPECIFICACIONES TÉCNICAS DEL ÍTEM Nº 01 Y DEL PLAN DE ENTREGAS DEL PRESENTE LLAMADO, LOS CUALES SE EXTIENDEN DE LA SIGUIENTE MANERA.

1. Especificaciones Técnicas

➢ ITEM Nº 01 – SERVIDOR TIPO RACKEABLE

Descripción Técnica Solicitada		Mínimo Exigido
Marca	-	Exigido
Modelo	-	Exigido
Chasis	Montaje en rack (1U).	Exigido
Procesadores	2x Intel Xeon-B 3106 8-Core (1.70GHz 11MB L3 Cache) Processor Kit.	Exigido
Memoria	**64GB (4 x 16GB) 2666MHz RDIMM.**	Exigido
Almacenamiento	**3 x 2TB SATA 7200 RPM LFF 3.5 Carrier**	Exigido
Bahías de Crecimiento	**Como mínimo debe quedar libre una bahía para futura expansión.**	Exigido
Ranuras de Expansión 5oportadas	**Controladora que soporte raid 0,1,5,10.**	Exigido
Tarjeta de Red	Embedded 1Gb 4-port Ethernet Adapter.	Exigido
Sistema Operativo Soportado	Windows Server 2012 R2 (Más reciente versión) Windows Server 2016 (Más reciente versión) VMware ESXi 6.0 U3 VMware ESXi 6.5 and U1 upon release Red Hat Enterprise Linux (RHEL) 6.9 and 7.3 SU5E Linux Enterprise Server (SLES) 11 SP4 and 12 SP2	Exigido
Fuente de Alimentación	**Mínimo de 500 Watts Hot plug low.**	Exigido
Kit de Rakeo	Carriles deslizantes, con brazo de administración de cables.	Exigido
Accesorios	**Debe incluir kit de rakeo**	Exigido
Garantía	3 Años En Piezas / 3 Años En Mano De Obra / 3 Años De Garantía A Domicilio El Siguiente Día Laborable.	Exigido
Autorización	**Presentar autorización del Fabricante o distribuidor donde autorice a la empresa oferente a presentar la propuesta.**	Exigido
Instalaciones	El oferente deberá montar el Rack e instalar el equipo en la oficina de la convocante.	Exigido
Servicio Técnico	La marca ofertada deberá poseer al menos un (1) Centro Autorizado de 5ervicios (CA5) para dar inmediata respuesta ante eventuales fallas del equipo.	Exigido

Certificaciones	Certificado de calidad ISO 9001:2000 del fabricante del equipo.	Exigido
Sistema Antivirus	**Sistema Antivirus Corporativo con necesidad de implementación en un servidor de alta gama. Dicho Antivirus será administrado por medio de una consola administrativa. Vigencia de la licencia 2 (dos) años. Cantidad 200 equipos.** **REQUERIMIENTOS MÍNIMOS:** 1.1.1.El Proveedor debe de estar incluido en el Informe de Gartner denominado "Magic Quadrant for Endpoint Protection Platforms" dentro cuadrante de líderes en los últimos 5 periodos. 1.1.2.La solución debe disponer de una consola WEB (HTTPS) y/o MMC; 1.1.3.La Consola de Administración debe disponer de Compatibilidad con Windows Failover Clustering u otra solución de alta disponibilidad. 1.1.4.Capacidad de eliminar remotamente cualquier solución de antivirus (propia o de terceros) que esté presente en las estaciones de trabajo y servidores, sin la necesidad de la contraseña de remoción del actual antivirus. 1.1.5.Capacidad de instalar remotamente la solución de seguridad de endpoint en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory; 1.1.6.Capacidad de instalar remotamente la solución de seguridad en dispositivos móviles con OS Android utilizando estaciones de trabajo como intermediadoras, portal de Auto Servicio y/o Portal Google Play. 1.1.7.Capacidad de gestionar smartphones y tablets (Windows Phone, Android y iOS) protegidos por la solución de seguridad de Endpoint para dispositivos móviles; 1.1.8.Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de enviar remotamente cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes; 1.1.9.Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores; 1.1.10. Capacidad de importar la estructura de Active Directory para encontrar máquinas;	Exigido

		1.1.11. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.; 1.1.12. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos; 1.1.13. Capacidad de definir políticas de configuraciones ligadas a estructura de grupos del directorio Activo de Microsoft. 1.1.14. Capacidad de etiquetar dispositivos o grupos de dispositivos mediante rotúlalos personalizables. 1.1.14.1. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora en que el software fue instalado o removido. 1.1.14.2. Actualizaciones de Windows Updates instaladas 1.1.14.3. Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD 1.1.14.4. Vulnerabilidades de aplicativos instalados en la máquina 1.1.15. Capacidad de reconectar máquinas clientes al servidor administrativo más cercano, basado en reglas de conexión como: 1.1.15.1. Cambio de gateway; 1.1.15.2. Cambio de subnet DNS; 1.1.15.3. Cambio de dominio; 1.1.15.4. Cambio de servidor DHCP; 1.1.15.5. Cambio de servidor DNS; 1.1.15.6. Cambio de servidor WINS; 1.1.15.7. Aparición de nueva subnet; 1.1.16. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet; 1.1.17. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes; 1.1.18. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus;	

		1.1.19. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red; 1.1.20. Integración nativa con Sistemas SIEM QRadar, Arcsight y Splunk. 1.1.21. Debe tener documentación de la estructura del banco de datos para generar informes a partir de herramientas específicas de consulta de terceros (Crystal Reports, por ejemplo). 1.1.22. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes; 1.1.23. Capacidad de reportar vulnerabilidades de software presentes en las computadoras. 1.1.24. Capacidad de realizar inventario de hardware de todas las máquinas clientes; 1.1.25. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes; 1.1.26. Capacidad de diferenciar máquinas virtuales de máquinas físicas; 1.1.27. Consola de Administracion basada en roles y perfiles de acceso. 1.1.28. La solución deberá generar reportes gráficos imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. 1.1.29. La solución debe permitir el manejo flexible de la licencia de manera que puedan ser reasignadas en caso que cambie el equipo dentro de un periodo de tiempo configurable. 1.1.30. La solución debe de disponer de una herramienta nativa de Backup que permita salvaguardar todas las configuraciones y datos para una posterior recuperación de los mismos. 1.1.31. La consola deberá permitir delegar la administración basada en roles y ubicaciones geográficas permitiendo de esta forma delegar la administración según la estructura de seguridad corporativa. 1.1.32. Métodos de detección basados en: Firmas, Heurística, asistido por Nube de seguridad del proveedor y defensa proactiva. 1.1.33. La solución deberá contar con medidas de seguridad para el usuario de la	

	estación de trabajo, sea este el administrador de la red o de la pc no deje sin efecto la política de seguridad corporativa. 1.1.34. La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante. 1.1.35. Vigilia proactiva ante amenazas del día 0, exploits 1.1.36. Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) 1.1.37. Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc.) 1.1.38. Firewall con IDS 1.1.39. Autoprotección (contra ataques a los servicios/procesos del antivirus) 1.1.40. Control de dispositivos externos 1.1.41. Control de acceso a sitios por categoría 1.1.42. Control de ejecución de aplicativos 1.1.43. Control de vulnerabilidades de Windows y de los aplicativos instalados 1.1.44. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación; 1.1.45. Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas 1.1.46. Capacidad de verificar solamente archivos nuevos y modificados; 1.1.47. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo 1.1.48. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL); 1.1.49. Capacidad de verificar tráfico de ICQ, MSN, AIM y IRC contra virus y enlaces phishings 1.1.50. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings; 1.1.51. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;		

		1.1.52. Debe tener soporte total al protocolo IPv6; - En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe: - Preguntar qué hacer, o; - Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o; - Permitir acceso al objeto 1.1.53. Debe tener módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas 1.1.54. Debe tener módulo IDS (Intrusion Detection System) para protección contra port scans y explotación de vulnerabilidades de software. 1.1.55. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc), con posiibilidad de configuración por usuario o grupos de usuarios y agendamiento. 1.1.56. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc). 1.1.57. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo 1.1.58. El control de Aplicaciones debe disponer de un Modo de Bloqueo por defecto (Default Deny). 1.1.59. Debe disponer funcionalidad de prevención ante ataques de BadUSB, el cual solicite o no al usuario validación del nuevo dispositivo. 1.1.60. Métodos de detección basados en: Firmas, Heurística, asistido por Nube de seguridad del proveedor 1.1.61. La solución deberá contar con medidas de seguridad para el usuario de la estación de trabajo, sea este el administrador de la red o de la pc no deje sin efecto la política de seguridad corporativa 1.1.62. La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante 1.1.63. Debe tener módulo IDS (Intrusion Detection System) para protección contra	

		port scans y explotación de vulnerabilidades de software. 1.1.64. La solución deberá contar con protección Anti-Ransonware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas producido por un equipo remoto 1.1.65. La solución debe de disponer un módulo de protección de red que permita el bloqueo de equipos remotos ante una incidencia de seguridad detectada **Compatibilidad:** - Microsoft Windows 10 Pro x86 / x64 - Microsoft Windows 10 Enterprise x86 / x64 - Microsoft Windows 8.1 Pro x86 / x64 - Microsoft Windows 8.1 Enterprise x86 / x64 - Microsoft Windows 8 Pro x86 / x64 - Microsoft Windows 8 Enterprise x86 / x64 - Microsoft Windows 7 Professional x86 / x64 SP1 o superior - Microsoft Windows 7 Enterprise / Ultimate x86 / x64 SP1 o superior - Microsoft Windows 7 Professional x86 / x64 - Microsoft Windows 7 Enterprise / Ultimate x86 / x64 - Microsoft Windows Vista x86 / x64 SP2 o superior - Microsoft Windows XP Professional x86 SP3 o superior. - Microsoft Windows Embedded 8.0 Standard x64 - Microsoft Windows Embedded 8.1 Industry Pro x64 - Microsoft Windows Embedded Standard 7* x86 / x64 SP1 - Microsoft Windows Embedded POSReady 7* x86 / x64 - Microsoft Windows XP Professional SP3 - Microsoft Windows Server 2012 R2 (Todas las ediciones - Microsoft Windows Server 2008 R2 (Todas las ediciones)	

2. Plan de Entregas

El plazo de entrega será de 20 (veinte) días calendario contados a partir de la recepción de la orden de Compra emitida por la convocante.
La falta de entrega del o de los bienes y o/ servicios dentro del plazo previsto obligará a la Institución a la aplicación de multas.

C.P.N. Melanio Maciel
Técnico - Unidad Operativa de Contrataciones
Consejo de la Magistratura
Escuela Judicial del Paraguay