

**PODER JUDICIAL DE LA PROVINCIA DE
CORRIENTES**

DIRECCION GENERAL DE ADMINISTRACION

LICITACION PÚBLICA 04/09

MOTIVO: Adquisición de SOFTWARE ANTIVIRUS Y SOFTWARE BASE para los servidores y estaciones de trabajo del Poder Judicial.

FECHA DE APERTURA: Ha sido fijada para el día **21 de Octubre de 2009** a las **10,00 hs.**

LUGAR A REALIZARSE: En el Departamento Licitaciones y Compras – Dirección General de Administración – Carlos Pellegrini N° 894 – Corrientes, Capital.

PLIEGOS: Podrán ser adquiridos en el Departamento Licitaciones y Compras – Dirección General de Administración – Carlos Pellegrini N° 894 – Corrientes, Capital.

MAYORES INFORMES: Departamento Licitaciones y Compras del Poder Judicial sito en Carlos Pellegrini N° 894 – Ex Casa Lagrãña – Telefax 03783 -426429 – 476893 – www.juscorrientes.gov.ar

PRESUPUESTO OFICIAL: \$ 424.600 (PESOS: CUATROCIENTOS VEINTICUATRO MIL SEISCIENTOS).

VALOR DEL PLIEGO: \$ 425 (PESOS: CUATROCIENTOS VEINTICINCO).

CONDICIONES GENERALES PARA ESTE PLIEGO

1. Las cantidades de licencias del software solicitado, podrán variar en más o en menos, conforme los precios ofertados y la disponibilidad de las partidas presupuestarias del Poder Judicial de la Provincia de Corrientes.
2. Deberá poseer software que nos brinde información acerca del hardware y la configuración de software y también que permita hacer testeos para asegurarse el correcto funcionamiento del equipo.
3. En caso de presentarse una “actualización tecnológica” en los bienes y/o elementos que formen parte de la oferta para cualquier ítem y en cualquier momento anterior a la entrega definitiva de la totalidad de los bienes, el Proveedor deberá suministrar tales elementos actualizados, contando con autorización previa de la Dirección General de Informática del Poder Judicial de Corrientes, y sin que esto implique un cargo adicional para el Poder Judicial. Se entenderá que ha ocurrido una actualización tecnológica cuando se presente una nueva versión del mismo producto en el mercado, que reemplaza a este, o cuando un nuevo producto con características técnicas superiores -en la línea de productos ofrecidas por el proveedor a la generalidad de sus clientes- reemplaza al modelo requerido por el Poder Judicial de Corrientes.
4. El Proveedor podrá, según su conveniencia y sin costos adicionales para el Poder Judicial, entregar bienes más avanzados o con características superiores a las ofrecidas, siempre y cuando cuente con la aprobación previa de la Dirección General de Informática del Poder Judicial de Corrientes. En ningún caso el Proveedor podrá entregar bienes cuya producción este discontinuada por el fabricante.
5. De los productos de software de la presente licitación se deberán entregar: originales en soporte óptico, manuales originales, en sus cajas respectivas, con sus respectivas licencias y toda la documentación donde conste la cantidad de licencias adquiridas así como sus claves para descarga desde Internet cuando así correspondiere.
6. El software deberá ser entregado con todos los manuales originales, en sus cajas correspondientes, así como todo lo necesario para su funcionamiento.
7. La solución de antivirus licitada tiene por objetivo la protección perimetral endpoints y de servicios core de todo el parque informático y su operatoria diaria en todo el Poder Judicial de Corrientes, de forma automatizada.
8. La propuesta de la solución de antivirus deberá incluir:
 - Presentación de un cronograma de tareas para la implantación de la solución en toda la infraestructura informática del PJC en todo el ámbito provincial.
 - La solución e implantación ofertada deberá ser del tipo “llave en mano”, de tal forma que el oferente deba encargarse de la total compatibilidad y funcionamiento de la solución tomando como base el hardware y software (tanto en servidores como en estaciones de trabajo) ya existente y en funcionamiento en el PJC.
 - **Alcances de la implantación del oferente y tiempo estimado de la misma:** **Alcances:** se entenderá como “llave en mano” la implantación de la solución en todos los servidores que posea el PJC así como en dos (2) localidades

satélites a designar, de tal forma que se dará conformidad de la misma una vez que el PJC haya comprobado en forma satisfactoria que la solución funciona correctamente y es adaptable a la infraestructura del PJC (LAN, WAN y servidores). **Periodo:** se considerara un periodo de 15 días hábiles como el deseable para la implantación de la solución; cualquier extensión a dicho periodo deberá consensuarse con la Dirección Gral. de Informática.

- La definición de los alcances de la implantación que hará el oferente y el tiempo estimado, mínimo y máximo, de dicha implantación.
 - **Equipo de trabajo:** se deberá acompañar curriculum vitae de los integrantes del equipo de trabajo que el oferente ocupará en la implantación, con el fin de lograr que la solución quede correctamente funcionando sobre la infraestructura que actualmente está en producción en el PJC. Se deberá indicar además, la función que cada uno desempeñará y una vez establecida no podrán ser intercambiados ni reemplazados sin aceptación por escrito de las autoridades competentes del Poder Judicial de Corrientes.
 - La descripción detallada de las funcionalidades del software antivirus ofertado, que permita su evaluación y comparación.
 - Asistencia técnica, respuesta calificada a consultas, aclaración de dudas, sobre el / los software/s componente/s de la solución y su completa compatibilidad con el hardware ya existente que posea el PJC.
 - Apoyo técnico para aprovechar al máximo las posibilidades y funciones de la solución de software ofertada y la transferencia de conocimientos a los especialistas designados por el Poder Judicial de Corrientes, que administrarán la solución en el futuro.
 - La definición de los recursos entre ambientes y plataformas que sean necesarias contemplar.
 - La definición de la seguridad interna requerida.
 - La implementación de las metodologías, resguardos y recuperaciones automáticas que provea la solución.
 - La definición y documentación de los procesos de la solución.
9. La solución ofertada deberá superar las Pruebas de Aceptación.

CONDICIONES PARTICULARES

Artículo 1: Las ofertas deberán ser presentadas en pesos, libre de gastos de flete, acarreo y embalaje, los que correrán por cuenta del adjudicatario.

Artículo 2: El oferente deberá cotizar cada renglón por separado, sabiendo que el renglón constituye la oferta básica que deberá ser cotizada invariablemente o declarada como "NO COTIZADO". El oferente podrá presentar alternativas de ofertas en todos los renglones que desee, siempre y cuando lo haga en la parte básica.

Artículo 3: Se evaluarán como elementos favorables para el oferente todas las características que estén mejoradas respecto a lo solicitado, y que se encuentren descriptas según el artículo 4.

Artículo 4: Se deberán incluir todos los folletos técnicos explicativos de los elementos propuestos, para la correcta identificación y evaluación de sus

características. No se admitirá especificar simplemente “según pliego” como identificación de los productos ofrecidos.

Artículo 5: Se requiere para ser oferente, haber operado en el rubro, en la República Argentina. El Poder Judicial se reserva el derecho de exigir constancias de lo mencionado. Solicitamos Nota que deje Constancia que la Empresa Oferente ha llevado a cabo un Proyecto similar en los últimos 2 años. Nota Escrita con Nombre de la Empresa y Contacto.

Artículo 6: Cualquier costo por otro concepto o adicional que requiera la utilización de los productos deberá detallarse en forma separada.

Artículo 7: El oferente deberá declarar expresamente las relaciones contractuales que los vinculan a las empresas fabricantes de los productos. Deberá presentar una Nota donde conste que es el Soporte Técnico Oficial de la Marca que Ofrece con una Antigüedad mayor a 3 años en la zona (Corrientes-Capital y Resistencia-Chaco). La misma debe ser totalmente corroborable y real. Requisito indispensable.

Artículo 8: Se establece que el plazo de entrega de la solución será de 15 (quince) días hábiles a partir de la notificación de la adjudicación.

Artículo 9: La demora en el cumplimiento de las entregas según el plazo establecido en la cláusula anterior, dará lugar a la aplicación de una multa del uno (1%) por ciento sobre el valor del producto no entregado, por cada día de retraso. Se tendrá en cuenta causas por razones excepcionales; en tal caso se deberá consensuar con la Dirección Gral. de Informática.

Artículo 10: Se entenderá que todo aquello que por error, omisión o desconocimiento no haya sido mencionado o solicitado en este pliego, y que haga al correcto funcionamiento de los productos, deberá tenerse como mencionado, y el adjudicatario procederá a su provisión.

Artículo 11: El oferente deberá presentar un domicilio legal dentro de la zona (Corrientes-Capital y/o Chaco-Resistencia).

Artículo 12: El licitante se reserva el derecho de exigir un equipo ó software de muestra a los efectos de su evaluación, incluyendo todos los accesorios y componentes necesarios para su funcionamiento. En este caso la Dirección Gral. de Informática del PJC tomara un periodo de 15 días hábiles para poder dar una evaluación técnica objetiva de las ofertas presentadas.

Artículo 13: El plazo de garantía de los productos de hardware y software se especifican en el renglón correspondiente. El mismo debe ser como mínimo de 3 años (cuando correspondiere).

Artículo 14: Los elementos ofertados serán nuevos, sin uso, originales de fábrica y su fabricación no deberá encontrarse discontinuada (nuevos y sin uso significa que el organismo será el primer usuario de los equipos desde que estos salieron de la fabrica).

Artículo 15: Se proveerán todos los elementos necesarios para su puesta en funcionamiento.

Artículo 16: Durante el plazo de garantía de los productos, el adjudicatario deberá prestar el servicio técnico que corresponda para restaurar el servicio (reparación o reemplazo) en un plazo máximo de 48 horas hábiles, contadas a partir de la notificación del desperfecto.

Artículo 17: El servicio de garantía deberá estar disponible desde las 8 Hs. hasta las

18 Hs. todos los días hábiles del año. Debiendo contar con una asistencia telefónica tipo 0-800 durante las 24 horas.

Artículo 18: Durante el plazo de garantía, el tiempo de respuesta a los llamados deberá ser de 8 Hs. hábiles como máximo.

Artículo 19: Cada uno de los puntos denominados "Opcional/es" en estos pliegos de Condiciones Particulares y Técnicas, deberá ser cotizado en forma separada; el Licitante no se obliga bajo ninguna circunstancia a contratar estos bienes o servicios opcionales. Sólo lo hará en el caso que la relación costo/beneficio resulte conveniente a los fines de cumplir el objetivo establecido. Sin embargo, la no cotización de estos opcionales o la cotización parcial de los mismos, podrá determinar la desestimación por parte del Licitante de la oferta completa.

Artículo 20: Deberá acreditarse en forma fehaciente que la solución este certificada por al menos un laboratorio de certificación independiente de nivel internacional (tipo ICASA, Checkmark, etc.). La solución ofertada deberá incluir un listado de compatibilidad de todo el software base y motores de DB en donde pueda ser instalada. La misma deberá ser full compatible y adaptable a la plataforma de hardware y servicios que posee el PJC en funcionamiento. Con adaptable se pretende que el impacto que resulte de la implantación de la solución sea mínimo o nulo y no afecte a los aplicativos y servicios que estén en correcto funcionamiento. A tal fin el oferente deberá tomar como referencias de la plataforma del PJC lo que indican: la "**Matriz de Compatibilidad de HW & SW**" (ver **ANEXO I**), el diagrama de la **Arquitectura de Red** (ver **ANEXO II**) y la **Matriz de Especificaciones Técnicas** (ver **ANEXO III**).

Artículo 21: Para cualquier consulta técnica los oferentes pueden dirigirse a la Unidad Ejecutora de Proyectos (U.E.P.), sito en Carlos Pellegrini 934 o bien a la dirección uep@juscorientes.gov.ar.

Artículo 22: El fabricante deberá proveer una herramienta de restauración local (tanto para estaciones de trabajo como para el server) que posibilite que el sistema pueda ser restaurado a un estado a salvo conservando los archivos.

Artículo 23: El fabricante deberá proveer una herramienta de diagnóstico local que brinde información acerca de la configuración de hardware y de software y cualquier otra información relevante que sirva a los fines de administración del equipo.

Artículo 24: En el caso que el oferente no sea el fabricante de lo cotizado, deberá presentar nota del fabricante original del mismo, ya sea de su sucursal local o de la casa matriz, en la que se certifique su carácter de representante oficial, distribuidor o vendedor autorizado, adjuntando documentación de respaldo. La documentación de respaldo deberá ser suficiente para acreditar la condición invocada y deberá estar certificada ante Escribano Público como prueba de autenticidad. En caso que se presenten contratos en idioma extranjero se deberá adjuntar traducción al español, efectuada por traductor público inscripto.

La mencionada representación deberá acreditar un plazo de efectiva vinculación comercial no menor a 12 (doce) meses en la República Argentina.

Artículo 25: El servicio de soporte "post venta" (garantía y soporte técnico) deberá ser de 3 años con un tiempo de respuesta no mayor a 48 horas durante las 8 horas los 5 días hábiles de la semana (5x8); adjuntándose a tal efecto el certificado de servicio correspondiente del fabricante, si así correspondiere.

Artículo 26: La solución deberá cotizarse para un periodo de 3 años en donde se incluirán todos los servicios, actualizaciones, soporte y garantía necesarios para que durante ese periodo la misma funcione sin mayores inconvenientes, salvo los de origen azaroso en cuyo caso corre lo estipulado en el artículo 25. Todo esto no deberá insumir costo alguno para el PJC durante ese periodo.

Artículo 27: La solución ofertada deberá además, considerar que la plataforma de servidores del Poder Judicial de Corrientes, en su mayoría, está montada sobre sistemas operativos Linux SUSE Enterprise Server (SLES versiones 9 & 10).

Artículo 28: La oferta deberá incluir necesariamente una capacitación para todo el equipo técnico del Poder Judicial de Corrientes que contenga los siguientes puntos como mínimo:

- Instalación
- Administración
- Soporte y solución de problemas
- Informes y reportes.
- Documentación impresa

Artículo 29: Las evaluaciones se realizarán de acuerdo con la **Matriz de Especificaciones Técnicas** (ver **ANEXO III**) y la **Matriz de Ponderación** (ver **ANEXO IV**) que se adjuntan al final del presente pliego. Es condición indispensable para el PJC el cumplimiento de los nueve (9) primeros ítems de la columna denominada “categoría”. El cumplimiento de esta condición asegura mínimamente que la solución ofertada será completamente adaptable y compatible con la infraestructura de red y servicios ya en funcionamiento en el PJC.

REGLON 01: SOLUCION DE SEGURIDAD PERIMETRAL ANTIVIRUS / ANTISPYWARE / ANTIMALWARE CORPORATIVO

Como parte de la licitación este renglón tiene por objetivo adquirir una solución de seguridad corporativa que conste de una herramienta de protección antivirus / antispymware y su servicio de soporte. Dicha protección se instalara en los puestos de trabajo y equipos servidores conectados a la red LAN y WAN como así también en equipos sin conexión a la misma. La solución se aplicará a todo el Poder Judicial de Corrientes, con el fin de realizar chequeos sobre todos los archivos, servicios, tráfico, etc. para la detección de código malicioso en la operatoria diaria y en forma automatizada.

Otro objetivo a lograr con la implementación de la solución, es que a través de las consolas de administración (en los Datacenters), se pueda controlar, visualizar, realizar los trabajos de actualización (firmas y programa), etc. tanto de Capital como del Interior, de tal forma que de ser necesaria la comunicación, la misma se realice desde el servidor local correspondiente y así evitar el envío de los datos de control / actualización por los otros enlaces de transmisión (MPLS/IP) alternativos debido a los anchos de bandas que se requerirían.

La infraestructura actual del PJC se conforma de cerca de 1700 estaciones de trabajo y de 38 servidores, distribuidos entre un (1) sitio central (Capital) y 4 cabeceras de circunscripción remotas (Interior). El diseño de la red WAN del PJC

tiene la arquitectura de servidores centrales (cabeceras) que ofrecen servicios locales y a sitios remotos (satélites). Para mas detalle ver el diagrama del **ANEXO II “Arquitectura de Red”**.

Especificaciones particulares y/o técnicas

Objeto de la contratación: adquisición de 1700 licencias antivirus, antispam y firewall personal y la correspondiente capacitación y operación para el número de personas que la Dirección Gral. de Informática determine. La misma deberá incluir: instalación, configuración, administración, soporte y solución de problemas, reportes e informes.

- El producto debe brindar protección integrada contra códigos maliciosos (virus, troyanos, spyware, adware, phishing, etc.), debiendo esa capacidad estar certificada por ICSA y/o Checkmark (West Coast Labs) u otra certificadora independiente de nivel internacional. Si el mismo motor de antivirus es utilizado en todas las versiones, es suficiente presentar el certificado de una sola versión.
- Se requiere que el producto haya sido sometido a auditorias realizadas por laboratorios independientes como ser Virus Bulletin, durante un periodo de al menos los últimos doce meses, sin tener ninguna falla en la detección de los Virus “In the Wild”, y sin haber emitido ningún falso positivo.
- El producto debe incluir antivirus, antispam y firewall personal brindando protección integrada contra códigos maliciosos (virus, troyanos, spyware, adware, phishing, etc.).
- Debe tener soporte para equipos con plataformas Windows de 32 y 64 bits.
- El servicio de soporte “post venta” (garantía y soporte técnico) deberá ser de 3 años con un tiempo de respuesta no mayor a 24 horas (contadas a partir de la notificación del desperfecto) durante los 5 días hábiles de la semana en horarios comerciales (8x5); adjuntándose a tal efecto el certificado de servicio correspondiente del fabricante, si así correspondiere. El plazo de incumplimiento no deberá exceder las 72 hs desde el reporte del incidente.
- Deberá tener representación y soporte técnico oficial radicado en el país con soporte telefónico, por mail y página Web donde se pueda abrir una incidencia.
- El oferente deberá acreditar soporte técnico en la zona (Corrientes-Capital y Resistencia-Chaco). La misma debe ser totalmente corroborable y real. Requisito Indispensable.
- La solución deberá cotizarse para un periodo de 3 años en donde se incluirán: todo el licenciamiento, mantenimiento, upgrade de servicios, soporte y garantía necesarios para que durante ese periodo la misma funcione sin mayores inconvenientes, salvo los de origen azaroso. Todo esto no deberá insumir costo alguno para el PJC durante ese periodo.

Administración de la Solución

- Deberá disponer de una/s consola/s de administración centralizada que permitan visualizar globalmente, de una manera resumida y en tiempo real, el estado de

los equipos protegidos por la solución, con al menos la siguiente información: versión de archivo de firmas, versión del antivirus o producto instalado, nombre de la máquina, IP, MAC, sistema operativo instalado, últimos eventos detectados, etc.

- La consola de administración deberá tener la posibilidad de ser accedida desde distintos lugares de la red, en forma segura.
- El producto debe permitir la creación de paquetes de instalación con configuración personalizada.
- Posibilidad de creación de múltiples perfiles de administración otorgando distintos permisos o privilegios incluyendo la posibilidad de crear un usuario que solo efectúe consultas o reportes.
- Posibilidad de creación de franjas horarias para tareas de actualización de firmas y paquetes para rangos de equipos.
- La administración centralizada no debe requerir un servidor dedicado.
- Instalación remota de las estaciones de trabajo.
- Permitir que los usuarios administradores de IT puedan acceder y modificar la configuración AV de la estación de trabajo y/o desde la consola de administración.
- No permitir cambio de las configuraciones del antivirus por parte del usuario común de la estación de trabajo.
- Permitir la creación de informes dinámicos y en tiempo real del estado de toda la solución, detecciones, actualizaciones y desinfecciones, etc.

Para Las Estaciones de Trabajo

Requerimientos de sistema

Procesadores compatibles:

- 32 bits (x86) y 64 bits (x64) Intel, AMD o 100% compatible.
- Sistemas operativos:
 - Microsoft Windows 2000.
 - Microsoft Windows XP (ediciones 32 y 64 bits)
 - Microsoft Windows Vista (ediciones 32 y 64 bits)
 - Microsoft Windows Server (ediciones 32 y 64 bits)
 - Soporte para el futuro Windows 7
- Tener bajo impacto en los recursos del sistema con una interfase compacta e intuitiva.
- Ejecutarse en equipos PC con mínimo impacto en el rendimiento del equipo, no debiendo producir una degradación superior al 20%.
- Autodefensa: poseer tecnología integrada con el fin de prevenir la corrupción o la desactivación de los sistemas de seguridad del sistema por parte de software malicioso.
- Deberá ofrecer un sistema que permita al usuario crear medios de recuperación de equipos infectados en un CD o memoria USB para poder arrancar el sistema desde los mismos y en forma limpia.

- Tener control de acceso de medios extraíbles, como memorias USB, CDs o discos de memoria flash, bloqueando esta potencial puerta a la infiltración de malware.
- Actualizaciones: en forma automática, programada o bajo demanda, en forma incremental, con mínimo impacto en el tráfico. Posibilidad de utilizar servidores en cascada en el proceso de actualización de tal forma de poder determinar el orden de búsqueda de los repositorios en caso de no encontrarse uno disponible (Ej., Rep1, Rep2, ...,Internet)
- La detección debe realizarse en forma preventiva, antes que el código malicioso se esté ejecutando en el equipo. Deberá poseer protección ante amenazas desconocidas y nuevos virus mediante el uso de heurísticas.
- Posibilidad de desinfectar, eliminar, renombrar el archivo infectado.
- Instalación, configuración, actualización y administración centralizada, remota y desatendida, con emisión de alertas en caso de detección de virus, equipos con antivirus no instalado o desactualizado, etc.
- Impedir a los usuarios que puedan desinstalar ni bajar de memoria la protección antivirus.
- Protección contra código malicioso oculto dentro del sistema operativo (rootkits).
- Detección de software malicioso (virus), software espía (spyware), programas de propaganda (adware), herramientas de hacking, programas discadores y mensajes de correo electrónico que reducen la productividad (SPAM, hoax y jokes), phishing y pharming en tiempo real.
- Es necesaria la integración con productos de mensajería instantánea (MSN, Windows Live Messenger, AOL, y Yahoo Messenger, PSI) analizando los archivos antes de que se escriban en disco.
- Análisis de tráfico HTTP entrante antes de que los archivos se escriban en disco y memoria.
- Posibilidad de almacenamiento de logs.
- Integración del anti-spam con clientes Outlook, Outlook Express, Thunderbird, y cualquier otro cliente de correo.
- Detección de phishing y pharming en cualquier cliente de correo.
- Analizar y detectar virus en archivos compactados y anidados, virus de arranque, virus de archivos, virus macros, virus de VB script y java script.
- Compatibilidad para análisis de archivos de formatos Microsoft Office.
- Posibilidad de análisis manuales y programados de las estaciones de trabajo.
- Protección contra virus de red (network virus) integrado en el cliente antivirus, tanto para estaciones como para servidores. Deberá incluir firewall en el puesto de trabajo.
- En caso de detección de archivos sospechosos, permitir el envío de alertas.
- Compatibilidad e integración con NAC (Network Access Control de Cisco).
- La solución deberá estar desarrollada en el idioma español.

Protección para servidores Linux

La solución deberá permitir proteger servidores Linux. Para detalles a cubrir se deberá consultar la **Matriz de Compatibilidad de HW & SW del ANEXO I**.

Especificaciones técnicas

- La solución deberá poder brindar protección al servidor WEB y proteger a los protocolos HTTP y FTP. Deberá permitir explorar todo el tráfico WEB entrante y saliente. Deberá proteger a todos los servicios que generen tráfico HTTP, HTTPS y FTP, tales como Squid y Apache dentro del servidor.
- La solución deberá brindar protección al servidor de correo electrónico, permitiendo el escaneo del tráfico entrante y saliente generado por el servicio Postfix dentro del servidor.
- La solución deberá proporcionar control de acceso de archivos sobre Samba. Deberá proveer protección contra todo tipo de malware para los servidores de archivos Linux tanto en exploración bajo demanda como en acceso debido al monitoreo y control en tiempo real del sistema completo de archivos. Analizar proactivamente comportamiento malicioso en los archivos para identificarlos como virus, spyware, adaware, troyanos, rootkis o cualquier tipo de código malicioso. Análisis heurístico capaz de detectar cualquier tipo de malware en el momento de su aparición.
- Deberá dar soporte a múltiples procesadores.
- Deberá ser compatible con plataformas de 64 bits.
- Análisis heurístico en los servidores Linux SLES (archivos y carpetas).
- Actualización automática de firmas y de forma incremental.
- Horarios de actualización configurables.
- Administración a través de interfaces gráficas.
- Generar alertas por e-mail (SMTP).
- Permitir realizar análisis inmediatos o programados en el servidor Linux.
- Posibilidad de realizar exclusiones en carpetas o archivos del sistema de archivos Linux.

EVALUACIÓN DE OFERTAS

Matriz de Especificaciones Técnicas – Matriz de Ponderación

Para obtener una correcta valorización será imprescindible que el oferente incluya una descripción completa de los productos y todo detalle que consideren relevante a los efectos del posterior estudio e indicar explícitamente la vigencia de las licencias solicitadas.

Con fines de unificar los criterios de evaluación, se adjuntan dos matrices en donde se detallan necesidades técnicas y valoración de las mismas respectivamente.

En la **Matriz de Especificaciones Técnicas** (ver **ANEXO III**) se presentan las 17 categorías a evaluar, las cuales se describen en forma detallada y de acuerdo a

la infraestructura y necesidades del PJC. Estos serán los puntos relevantes que la solución ofertada deberá cubrir.

La misma deberá ser completada en el campo "NOTAS", especificando con las siguientes leyendas:

- * **"Cumple"**, para los casos donde se cumpla la totalidad del requerimiento
- * **"No Cumple"** para aquellos donde no se cumple ó,
- * **"Cumple Parcialmente"**.

En caso de cumplirse total o parcialmente se deberá especificar el nivel de cumplimiento que se tenga agregando un detalle de funcionalidades y características en el renglón correspondiente.

En la **Matriz de Ponderación** (ver **ANEXO IV**) figuran las 17 categorías mencionadas, divididas en dos secciones. Cada sección tendrá una valoración porcentual que representa el nivel de importancia relativa que le asigna el PJC a cada una de ellas.

Dentro de cada sección, se ponderará el peso relativo de cada característica técnica evaluada, a las cuales se le asignará un puntaje.

Nota: en cada sección y entre paréntesis figurara el factor de ponderación que se utilizara para cada caso.

Las 2 secciones a ser evaluadas son:

1º Sección: Características indispensables (90%): incluyen a las primeras 9 categorías evaluadas, es **condición indispensable** para el PJC que estas sean cumplimentadas por la solución ofertada dado que ellas afectan directamente a la infraestructura y operatoria normal del PJC.

Requisitos mínimos de funcionalidad: para que la solución ofertada pueda ser considerada como tal deberá satisfacer al menos 70 puntos (ya ponderados) de las características indispensables, caso contrario la solución será desestimada por no cumplir con el mínimo necesario.

2º Sección: Características deseables (10%): incluyen las demás categorías (10 a 17), las cuales son requisitos altamente deseables para el PJC.

En caso de incumplimiento de alguna de las 17 categorías quedará a criterio de la Dirección Gral. de Informática la evaluación sobre el impacto que podría tener dicho evento sobre la infraestructura del PJC.

En la evaluación técnica de la propuesta de los oferentes, el PJC le asignara el total del puntaje de una determinada característica si **"Cumple"** totalmente dicho ítem; se le asignará la mitad del puntaje si **"Cumple Parcialmente"** o no se le asignará puntos si el oferente **"No Cumple"** el ítem evaluado.

Puntaje Técnico (PT)

El puntaje técnico de la oferta resultará de la sumatoria de los puntos obtenidos en las distintas características multiplicado por su factor de ponderación correspondiente.

$$PT = \sum (\text{Puntos} \times \text{Ponderación} / 100)$$

Puntaje Económico (PE)

Se otorgará 100 puntos al precio más bajo de las ofertas que según la evaluación técnica realizada por el PJC cumplan los requisitos mínimos de funcionalidad. El puntaje de cada una de las demás ofertas clasificadas se obtendrá dividiendo el precio de la oferta mas baja por el precio respectivo de cada oferta y multiplicado por 100.

Puntaje Final (PF):

$$PF = PT + PE$$

El puntaje final de la oferta resultará de sumar el puntaje técnico obtenido más el puntaje económico.

REGLON 02: SOLUCION DE SOFTWARE BASE

En concordancia con la solución de seguridad ofrecida en el Renglón 01, el PJC tiene como objetivo en este renglón la adquisición del software base (sistema operativo y motor de base de datos) que sirva como plataforma de software para los equipos de core que gestionaran y administraran la solución corporativa pretendida, para toda la arquitectura de red provincial, así como de otros servicios proyectados. Tomando como referencia los **ANEXOS I, II y III** se pretende una solución de software base que sea full compatible con plataformas Windows Server y SQL Server.

Para el licenciamiento de dichos productos se tomará en cuenta lo siguiente:

- El gran tamaño del parque informático y que cada equipo cliente se conectará a una base de datos
- Que el PJC ya dispone de servidores con poca cantidad de procesadores pero con CPUs multinúcleo y de alto rendimiento.
- Que como consecuencia de los anteriores sería conveniente cotizar licencias a nivel de los procesadores y no de la cantidad de clientes o dispositivos que lo accedan.
- Tomando en cuenta la infraestructura de red del PJC, se deberían cotizar 1 (una) licencia de Windows Server 2008 x64 Enterprise Edition para el servidor

- principal de la infraestructura y 4 (cuatro) licencias de Windows Server 2008 x64 Standard Edition para los 4 (cuatro) servidores del interior de la provincia.
- Tomando en cuenta la infraestructura de red del PJC, se deberían cotizar 5 (cinco) licencias de SQL Server 2008 x64 Standard Edition para el servidor principal de la infraestructura y los cuatro servidores del interior de la provincia.
 - Preveer para la cotización un esquema diferenciado de precios de licencias para gobierno, de tal manera de que el PJC pueda obtener contratos con términos y precios especiales.
 - Todos los productos cotizados tengan la leyenda "GOV".
 - Gestión de licencias fácil y poco costosa y la posibilidad de agregar licencias en la modalidad de pago por uso para nuevas compras.
 - Ser parte del programa de licencias por volumen de Microsoft para organizaciones gubernamentales.

Condiciones particulares para el oferente

- Para cada uno de los ítems de software el oferente deberá acreditar experiencia en la comercialización y/o venta de licencias Microsoft, para lo cual anexará a su propuesta un mínimo de tres (3) certificaciones de contratos de licenciamiento ejecutados en los últimos años.
- Las certificaciones deberán contener: fecha de inicio, fecha de terminación, y valor total ejecutado expresado en pesos. Así mismo, deberán ser expedidas por la entidad pública o privada contratante.
- Se requiere que el oferente acredite como mínimo la condición de **Certified Partner de Microsoft**, expedida por el fabricante y vigente. Se valorará especialmente aquellos oferentes que acrediten el nivel **Gold Certified Partner**. Adicionalmente se requerirá al oferente que detalle en su propuesta las competencias en las cuales se encuentra certificado.
- Con el fin de asegurar que la oferta está en un todo de acuerdo con los términos de licencia del fabricante, y se ajusta a las necesidades del organismo, se requiere al oferente de manera obligatoria, tener registrado ante el fabricante, profesionales certificados en MCSE, MCP ó MCTS, todos con credenciales y experiencia en implementaciones en Microsoft Windows Server y SQL Server. Para la oferta de licencias de Microsoft SQL Server, se requieren certificaciones MCITP sobre dicho producto.
- Preferentemente el oferente deberá tener casa central o sucursal en la ciudad de Corrientes.
- Soporte post-venta (garantía y soporte técnico) sobre el producto ofertado tanto por el fabricante como por el proveedor.

ANEXO I - MATRIZ COMPATIBILIDAD HW & SW

PODER JUDICIAL DE LA PROVINCIA DE CORRIENTES

DPTO. ANALISIS DE REDES, SOPORTE TECNICO Y TELECOMUNICACIONES

Servidores Criticos a Proteger

| Cant. | Tipo de Servidor | Sistema Operativo - x64 | Cantidad Procesadores | Version Nucleo |
|-------|------------------|----------------------------------|-----------------------|---|
| 8 | HP ML370-G4 | SLES10-SP1 | 2 - SCore 3.6Ghz | Kernels: 2.6.xxx-smp |
| 2 | HP ML370-G4 | SLES9 | 2 - SCore 3.6Ghz | Kernels: 2.6.xxx-smp |
| 3 | HP ML370-G5 | SLES10-SP1 | 2 - Qcore 2.3Ghz | Kernels: 2.6.xxx-smp |
| 6 | HP ML370-G5 | SLES9 | 2 - Qcore 2.3Ghz | Kernels: 2.6.xxx-smp |
| 10 | HP DL320-G5 | SLES10-SP1 | 1 - Dcore 2.4Ghz | Kernels: 2.6.xxx-smp |
| 4 | HP ML370-G5 | SLES10-SP1 | 2 - Qcore 2.3Ghz | Kernels: 2.6.xxx-smp |
| 4 | HP DL160-G5 | WinSrvStd 2008 + SQL SrvStd 2008 | 1 - Qcore 2.0Ghz | Servidores AV Secundarios a implementar |
| 1 | HP ML370-G5 | WinSrvEnt 2008 + SQL SrvStd 2008 | 2 - Qcore 2.3Ghz | Servidor AV Central a implementar. |
| 38 | | | | |

Estaciones de trabajo a Proteger

| Cant. | Tipo de PC | Sistema Operativo | Cantidad Procesadores | Memoria |
|-------|------------------|--|------------------------------|----------|
| 1700 | HP DX2000MT | Windows XP 32 bits | 1 - PENTIUM IV 2,8 Ghz | 512 Mb |
| | HP DX5150MT | Windows XP 32 bits | 1- ATHLON 64 3500+ 2,2 Ghz | 512 Mb |
| | HP DC5750 | Windows XP 32 bits | 1- ATHLON 64 3500+ 2,2 Ghz | 512 Mb |
| | HP COMPAQ DC5850 | Windows XP 32 bits | 1- ATHLON X2 (4450B) 2,3 Ghz | 1 Gb |
| | Clon | Windows XP 32 bits / Windows 2000 pro | 1- CELERON 2,4 Ghz | 256 Mb |
| | Clon | Windows XP 64 bits / Windows Vista 64 bits | 1- PENTIUM CORE 2 Quad 2,66 | 4 Gb |
| | Notebook | Windows XP y Vista de 32 bits /64 bits | 1- PENTIUM CORE 2 Duo | 2 y 4 Gb |

Servicios sobre servidores Linux a proteger

| Cantidad | Servicio | SO Base |
|---------------------------------|-------------------------|------------|
| 1 Server de Mail (1200 mailbox) | Postfix 2.4.5-20.x | SLES10-SP1 |
| 6 Servidores Proxies | Squid 2.5.STABLE12-18.x | SLES10-SP1 |
| 6 Servidores Samba | Samba 3.0.28-0.x | SLES10-SP1 |
| 2 Servidores WEB | Apache 2.2.x | SLES10-SP1 |

Poder Judicial de Corrientes

ANEXO II - Arquitectura de Red Provincial

Arquitectura de la red provincial:

* El Poder Judicial de Corrientes (PJC) cuenta actualmente con 12 localidades conectadas a través de una red IP-MPLS.

* La arquitectura de red esta formada por un Datacenter central (Capital) y 4 Datacenters secundarios (interior de la Provincia); cada uno de los cuales es cabecera de circunscripción.

* De cada cabecera dependen una o mas localidades satélites.

* Todos los enlaces de la red full mesh son de 1 Mbps, provistas por un proveedor local de comunicaciones.

* Todas las localidades se encuentran enlazadas por medio de VPNs.

* Cada localidad posee una red MAN de FO conectando los edificios existentes.

Se desea:

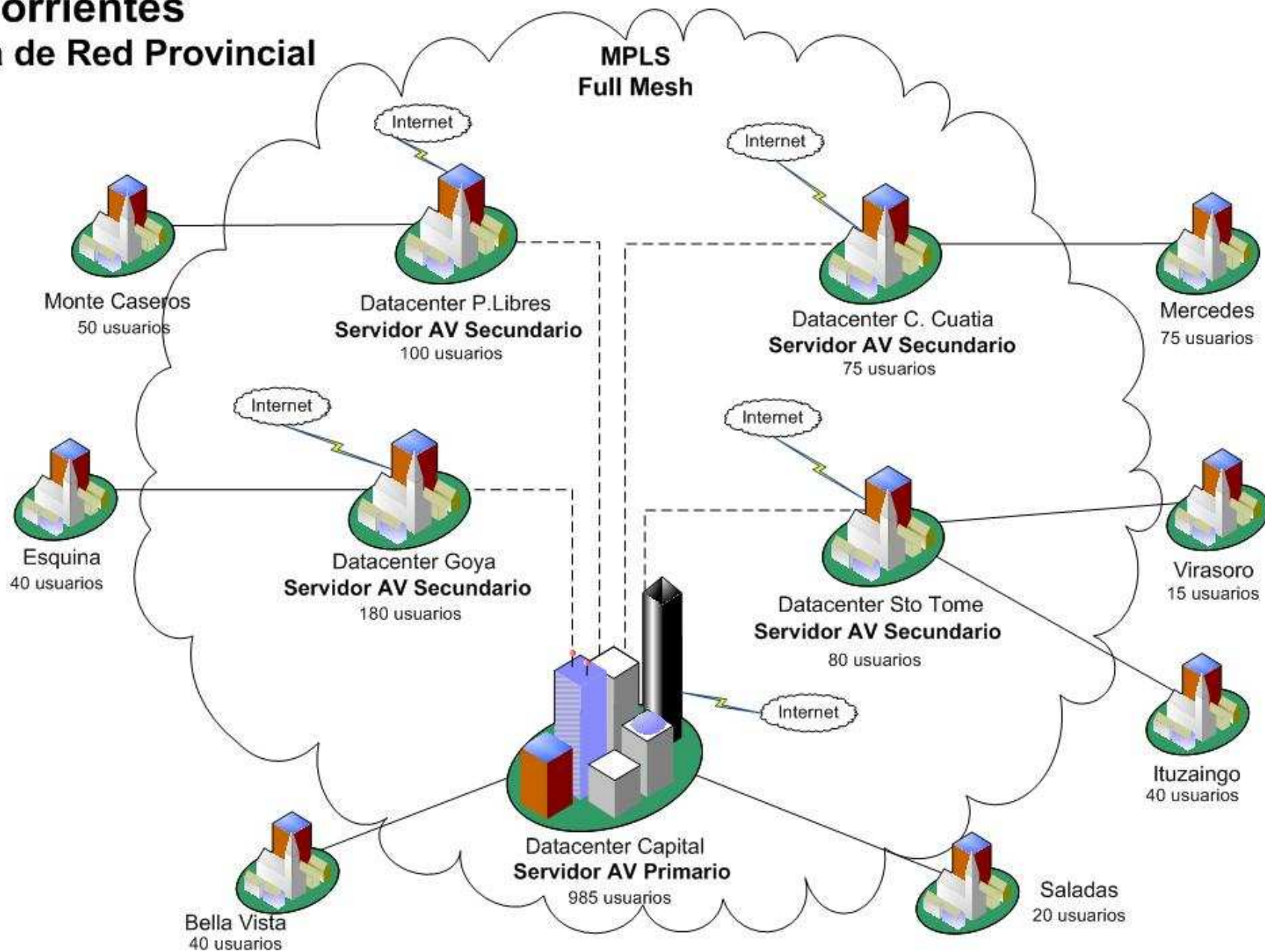
* Que en la localidad Capital se instale el servidor de Antivirus Primario, y en las cabeceras de circunscripción (Goya, Curuzu Cuatia, P. de los Libres y Santo Tome) los servidores AV secundarios.

Cada Datacenter (y solo ellos) tiene un enlace dedicado a Internet. El Datacenter capital tiene un enlace de 2 Mbps, y los del interior de 1 Mbps; por lo que los servidores tendrían de esta forma una conexión directa para actualizarse.

* Evitar tráfico de red innecesario hacia la Capital.

* Que cada servidor secundario pueda administrar todas las estaciones de trabajo de su circunscripción (locales y las de sus localidades satélites). Por ejemplo: el servidor del Datacenter Goya deberá manejar las estaciones de trabajo de dicha ciudad más las de la localidad de Esquina, es decir un total de 220 estaciones de trabajo (180 de Goya más 40 de Esquina).

* Que toda la información relevante se replique y esté disponible en el servidor primario de Capital a los fines de administración.



ANEXO III - MATRIZ ESPECIFICACIONES TECNICAS

PODER JUDICIAL DE LA PROVINCIA DE CORRIENTES

DPTO. ANALISIS DE REDES, SOPORTE TECNICO Y TELECOMUNICACIONES

| | Categoría a Evaluar | Notas |
|--------------------------------|---|-------|
| CARACTERISTICAS INDISPENSABLES | <p>1 <u>Arquitectura</u>. Segun esquema adjunto, se tendrá un servidor central en Capital y servidores secundarios en los 4 datacenter del Interior, los cuales realizarán toda la gestión y administración de las PCs de su circunscripción. Cada servidor secundario deberá poder mandar periodicamente información resumida del estado de sus clientes hacia el servidor central de capital (en forma automática o a pedido y solo ese tipo de información) de modo de poder tener un control centralizado del estado del parque. Se pretende una arquitectura con servidores distribuidos minimizando el tráfico hacia la Capital. De igual forma se pretende que el tráfico entre las localidades satélites y su cabecera origen sea mínimo (se considerará tráfico: actualización de definiciones, actualizaciones de programa, información de control, etc el cual además de ser mínimo deberá permitir programación por franjas horarias para dichos eventos). Se deberá evaluar el peor caso en el uso de los enlaces WAN de transmisión, es decir cuando un grupo de estaciones reciban concurrentemente paquetes desde su server central. Para más detalle ver el gráfico de la red provincial del PJC.</p> <p>De ser necesario la solución deberá permitir escalar a través de la instalación de repositorios de actualización en las localidades satélites.</p> <p>El diseño de la solución que se presente no deberá, en ningún caso, implicar cambios en el diseño y configuración de la red ya implementada en el PJC.</p> | |
| | <p>2 <u>Protección para servidores Linux</u>: La solución deberá permitir escaneo del tráfico generado por los servicios Samba, Postfix, Squid, Apache, dentro del servidor.</p> | |
| | <p>3 <u>Funcionamiento</u>: La solución deberá funcionar con todas las protecciones activas (sin sacrificar ninguna de sus funcionalidades). Es condición indispensable que la solución haga un uso mínimo de los recursos de la PC (procesador y memoria) sin afectar mayormente el óptimo desempeño de la estación de trabajo (sobre todo el de las aplicaciones críticas utilizadas en el PJC). No se desea una degradación de la performance del sistema mayor a un 20 %.</p> <p>Referencia: equipos Pentium IV 2.8 Ghz / Athlon 2.2 Ghz - RAM 512 MB</p> | |
| | <p>4 <u>Contingencia</u>: se deberá proveer una herramienta de recuperación / restauración ante falla de/los servers AV. Deberá permitir realizar backups/restore de la DB, paquetes, configuraciones y storage del server. La función de restauración deberá permitir volver al estado normal, anterior a la falla, de tal manera que el evento de falla haya sido transparente para los clientes y el administrador, conservando las configuraciones y perfiles utilizados.</p> | |
| | <p>5 <u>Administración del Cliente</u>: La solución deberá permitir que los administradores de IT puedan utilizar todas las funcionalidades de configuración en la estación cliente y en forma standalone (ante fallas o a los fines de soporte y mantenimiento) y/o desde las consolas de administración. Para lograr tal funcionalidad es menester que en la estación de trabajo la solución AV requiera a los usuarios avanzados de IT algún tipo de autenticación de seguridad.</p> | |
| | <p>6 <u>Funcionalidades</u>: La solución deberá ofrecer las mismas funcionalidades (antivirus, antispyware, antimalware, firewall y antisпам), o la mayoría de ellas, tanto en la estación de trabajo como en los servidores, tanto para arquitecturas de 32 como de 64 bits, y para cualquier plataforma Windows que se utilice.</p> | |
| | <p>7 <u>Sistema operativo base (server primario y secundarios)</u>: se requerirá que la solución corra sobre plataformas Windows Server x64 en todos los puntos de cabecera (Capital e interior) dada la limitación inherente de las conexiones concurrentes de los windows de escritorio.</p> <p>De la misma forma se requiere que la solución corra con Microsoft SQL Server 2008 para todos los puntos centrales con el fin de garantizar una solución robusta y escalable.</p> | |
| | <p>8 <u>Integración / control de aplicaciones (ofimáticas, browsers, clientes de correo, etc.)</u>: la solución deberá integrarse completamente con cualquier cliente de correo electrónico, de navegación como así también paquetes ofimáticos. Deberá ofrecer protección en tiempo real a nivel de protocolos de comunicación (análisis de tráfico) con posibilidad de creación de políticas de control de aplicaciones (permitir o denegar).</p> | |
| | <p>9 <u>Soporte Técnico</u>: deberá ser de 8x5 y en español, preferentemente con representación local.</p> | |
| CARACTERISTICAS DESEABLES | <p>10 <u>Modalidad de licenciamiento del producto</u>: la totalidad de la solución deberá proveerse por un período de 3 años para la cantidad de usuarios, servidores, estaciones de trabajo y mailbox en todos los Datacenters que el PJC posea, sin importar la posible variación de sistemas operativos o cantidad de Datacenters, de tal forma que en caso de aumentar la cantidad de estaciones de trabajo y/o mailbox se puedan adicionar licencias.</p> | |
| | <p>11 <u>Idioma del Producto</u>: deberá ser en español.</p> | |
| | <p>12 <u>Simplicidad / velocidad de uso GUI Server</u>: la solución deberá poseer una interfase amigable e intuitiva con posibilidad de uso de asistentes y con una curva de aprendizaje corta.</p> | |
| | <p>13 <u>Reportes / Información estadística</u>: la solución deberá permitir la generación de informes personalizados para conocer el estado de los equipos, grado de infecciones, estado de las protecciones, de detecciones, de actualizaciones, etc. Estos reportes deberán permitir la posibilidad de ser exportados a otros formatos (pdf, xml, html, etc) y de ser enviados vía mail. De la misma manera el servidor de administración deberá permitir la visualización del estado en tiempo real del parque y sus protecciones, permitiendo actuar proactivamente sobre posibles problemas.</p> | |
| | <p>14 <u>Desinstalación / Instalación remota</u>: la solución debería proveer la posibilidad de poder realizar la desinstalación remota de soluciones AV ya instaladas en el PJC (comerciales y/o gratuitas) y disponibles en el mercado. Se deberá especificar el funcionamiento de esta funcionalidad. De la misma forma la solución debería poder realizar instalaciones remotas de sus clientes.</p> | |
| | <p>15 <u>Creación de paquetes</u>: la solución deberá permitir crear paquetes de instalación (Exe, MSI, etc) con distintas protecciones e incluso con archivos de configuración personalizados para ser distribuidos de forma directa a las estaciones clientes y según perfiles de usuario.</p> | |
| | <p>16 <u>Garantía</u>: durante el período de licenciamiento la oferta deberá cubrir con actualizaciones del programa, de las firmas de nuevas versiones de soft, parches, y acceso a documentación técnica, todo en forma gratuita.</p> | |
| | <p>17 <u>Capacitación</u>: como parte de la solución se deberá cotizar un temario avanzado de capacitación con modalidad presencial on-site y para 10 personas. Será condición requerida la extensión de certificados de asistencia / aprobación.</p> | |

ANEXO IV - MATRIZ DE PONDERACION

PODER JUDICIAL DE LA PROVINCIA DE CORRIENTES

DPTO. ANALISIS DE REDES, SOPORTE TECNICO Y TELECOMUNICACIONES

| | Categoría a Evaluar | Ponderación de la seccion | Puntos | | |
|---|--|---------------------------|------------|-----------|-----------|
| | | | Cumple | Parcial | No Cumple |
| 1º SECCION Características INDISPENSABLES | | 90% | | | |
| 1 | Arquitectura | | 30 | 15 | 0 |
| 2 | Protección para servidores Linux | | 15 | 7,5 | 0 |
| 3 | Funcionamiento | | 15 | 7,5 | 0 |
| 4 | Contingencia | | 10 | 5 | 0 |
| 5 | Administracion del Cliente | | 10 | 5 | 0 |
| 6 | Funcionalidades | | 5 | 2,5 | 0 |
| 7 | Sistema operativo base (server primario y secundarios) | | 5 | 2,5 | 0 |
| 8 | Integracion / control de aplicaciones | | 5 | 2,5 | 0 |
| 9 | Soporte Tecnico | | 5 | 2,5 | 0 |
| | | | 100 | 50 | 0 |
| 2º SECCION Características DESEABLES | | 10% | | | |
| 10 | Modalidad de licenciamiento del producto | | 10 | 5 | 0 |
| 11 | Idioma del Producto | | 5 | 2,5 | 0 |
| 12 | Simplicidad / velocidad de uso GUI Server | | 5 | 2,5 | 0 |
| 13 | Reportes / Información estadística | | 15 | 7,5 | 0 |
| 14 | Desinstalación / Instalacion remota | | 15 | 7,5 | 0 |
| 15 | Creacion de paquetes | | 30 | 15 | 0 |
| 16 | Garantía | | 10 | 5 | 0 |
| 17 | Capacitación | | 10 | 5 | 0 |
| | | | 100 | 50 | 0 |
| TOTAL | | 100% | | | |