



PLIEGO DE ESPECIFICACIONES TECNICAS

RENGLON 01

SOLUCION DE SEGURIDAD PERIMETRAL – ANTIVIRUS / ANTISPYWARE / ANTIMALWARE CORPORATIVO

El Poder Judicial de Corrientes tiene por objetivo renovar la solución de seguridad corporativa la cual se fundamenta en una herramienta de protección antivirus / antispyware y su servicio de soporte.

La solución se aplicará a todo el parque informático en toda la Provincia, 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.

Tener en cuenta que la infraestructura actual y futura (con crecimiento) del PJC se conforma de cerca de 2500 estaciones de trabajo distribuidos entre 5 cabeceras de circunscripción (Capital e Interior). Se desea mantener la implementación actualmente vigente, la cual a través de consolas de administración distribuidas (en 5 Datacenters) se puede controlar, visualizar, realizar los trabajos de actualización (firmas y programas), etc, para todo el ámbito Provincial.

DESCRIPCION de la SOLUCION: debe proporcionar: protección inmediata contra amenazas desconocidas y avanzadas, detectar los ataques dirigidos con eficacia, protección de las amenazas más recientes y sofisticadas, incluidos los exploits. análisis de vulnerabilidades y administración de parches, seguridad multicapa, incluido el cifrado, control web, control de aplicaciones, control de dispositivos, seguridad y administración de dispositivos móviles y una consola para la de administración unificada y centralizada de la seguridad y los sistemas.

Debe incluir el conocimiento y las habilidades necesarias para que se descubran todas las funciones de la solución necesarias para la planificación, implantación, mantenimiento y optimización de la red Windows, administrar el sistema desplegado y gestionarlo a través de la consola de administración unificada.

Debe integrar, como mínimo, las siguientes funcionalidades y tecnologías en su plataforma de seguridad:

- **Protección:** debe poseer Anti-Malware y Firewall.
- **Control de Aplicaciones, de Dispositivos y de Web:** involucra una serie de funciones para controlar qué dispositivos pueden acceder a una red y con ello, proteger sus sistemas y datos
- **Cifrado de Datos:** la función de cifrado de datos, con políticas de seguridad altamente integradas que pueden alinearse con los controles de aplicaciones y dispositivos, protege los datos en caso de robo o extravío de archivos o dispositivos
- Seguridad en Servidores de Archivos.
- Seguridad de Endpoint Móvil (Tablets, Notebooks, Smartphones). Manejo de Dispositivos Móviles.
- Protección de Datos (Encriptación).

- Manejo de Licencias de Software, de Parches de Seguridad y Escaneo de Vulnerabilidades.
- Administración de Red (NAC).
- Instalación de software en forma remota. Imagen y aprovisionamiento de Sistemas Operativos.
- Permitir administración centralizada a través de consolas e incluir tecnologías asistidas a través de la nube Web.
- Debe tener soporte para equipos con plataformas Windows (XP, W7, W8, W10) de 32 bits (x86) y 64 bits (x64) Intel, AMD o 100% compatible.
- La solución debe estar desarrollada en idioma español.

CANTIDAD: renovación y adquisición de la licencia Kaspersky Endpoint Security for Business Advanced para 2500 nodos antivirus, antispam y firewall personal.

PERIODO a CUBRIR: la solución debe cotizarse para un periodo de 3 (tres) años en donde se incluirán: todo el licenciamiento, 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.

SOPORTE y GARANTIA: debe poseer representación y soporte técnico oficial radicado en el país con soporte telefónico, por mail y página web donde se pueda abrir una incidencia. Se pretende que como parte de la propuesta de la solución **se incluya solamente la asistencia técnica básica o soporte estándar** (la que viene incluida con la solución, sin ningún otro servicio adicional) permitiendo procesar errores que se presenten, realizar troubleshooting, procesar incidentes maliciosos, respuestas a consultas y aclaración de dudas, sobre los componentes de la solución. Cualquier otro tipo de soporte o servicio, adicional o extendido, deberá ser cotizado como alternativa, reservándose el Poder Judicial el derecho de aceptación según su conveniencia.

El servicio de garantía de soporte debe estar disponible todos los días hábiles del año desde las 8 Hs. hasta las 19 Hs (mínimo) debiendo contar con una asistencia telefónica, web (con tickets) o similar con un tiempo de respuesta no mayor a 48 (cuarenta y ocho) horas contadas a partir de la notificación del desperfecto.

REGLON 02

CAPACITACION

DESCRIPCION: con el fin de aprovechar al máximo todas las funcionalidades que brinda el nuevo producto el PJC pretende capacitar a su capital humano en relación al producto a adquirir y los requerimientos específicos que se necesitan cubrir en la infraestructura ya implementada.

CANTIDAD: debe ser del tipo "**Kaspersky KL 002.10, Kaspersky Endpoint Security and Management. Essentials**". Debe ser dictado en sitio del cliente y para un estimado de 8 (ocho) personas. El temario debe ser dictado tomando en cuenta el último producto disponible en el mercado y debe permitir adecuar los temas a las necesidades requeridas por el PJC-DGI con la finalidad de aprovechar al máximo



DIRECCIÓN GENERAL DE INFORMÁTICA
PODER JUDICIAL DE CORRIENTES
"AÑO DEL BICENTENARIO DE LA DECLARACIÓN DE LA INDEPENDENCIA NACIONAL"

sus funcionalidades. Debe ser dictado por un profesional certificado de la marca y debe dictarse en idioma español.