INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE
ANTIVIRUS CORPORATIVO
Nº 001-2014-OEI-HEP

1.- NOMBRE DE LA UNIDAD ORGÁNICA:

Oficina de Estadística e Informática

2. RESPONSABLES DE LA EVALUACIÓN:

Lic. Teodoro Zuasnábar Junes
Sra. Diana Lidia Requena Campoverde

3. CARGOS:

Director de Oficina de Estadística e Informática
Responsable del Equipo de Trabajo de Informática

4.- FECHA:

Viernes 28 de Febrero de 2014.

5.- JUSTIFICACIÓN:

Se requiere renovar las Licencias de Software Antivirus Corporativo con la finalidad de garantizar una adecuada protección de los sistemas informáticos y aseguramiento de la integridad de la información; lo que permitirá la continuidad de las labores y cumplimiento de las funciones de la institución.

6.- ALTERNATIVAS:

Entre las distintas opciones para adquirir un software antivirus en el mercado nacional y que tenga algunas o todas las características que requerimos, hemos evaluado las cuatro siguientes:

- ESET ENDPOINT SECURITY
- KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT
- GDATA ENPOINT PROTECCION BUSINESS
- THE HACKER

7.- ANÁLISIS COMPARATIVO TÉCNICO

a. **Propósito de la Evaluación.**
Determinar el Software Antivirus con las mejores características y atributos para su adquisición en bien de la protección de la data adquirida y/o generada por los sistemas usados en el Hospital de Emergencias Pediátricas.

b. **Identificación del Tipo de Producto**
Software Antivirus.

c. **Especificaciones del Modelo de Calidad.**
Se aplicará el modelo de calidad de Software descrito en la Guía de Evaluación de Software para la Administración Publica (Resolución MinisterialN°139-2004-PCM).

d. **Selección de Métricas.**
Las métricas han sido seleccionadas en base al análisis de las características técnicas alcanzadas por cada uno de los distribuidores de los productos seleccionados en el parte 6 del presente informe.

Métricas a tener en cuenta para la evaluación

ITEM	ATRIBUTOS	DESCRIPCION
ATRIBUTOS INTERNOS		
1	Sistemas Operativos Estaciones de Trabajo 32 y 64 Bits	Microsoft Windows XP Professional, Microsoft Windows 7. Microsoft Windows 8.
2	Sistemas Operativos Servidores de Red	Microsoft Windows 2003 Server Microsoft Windows 2008 Server Microsoft Windows 2012 Server
3	Actualizaciones	Manuales y automáticas (programadas) del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo desde Internet. Debe brindar la creación de repositorios distribuidos y programados.
4	Compatibilidad	Carta de fabricante del software antivirus indicando total compatibilidad con los sistemas operativos mencionados en las versiones anteriormente mencionadas.
5	Instalación	La instalación del software a los computadores de los usuarios debe ser debe ser directamente desde la consola de administración, además de la posibilidad de instalación mediante CD o recurso UNC. Para instalar de manera local la consola deberá permitir crear paquetes de instalación (oneclick) para una instalación rápida y sencilla obviando la instalación rutinaria. Desinstalación automática de otro software antivirus que tuviese el equipo al ser instalado el antivirus.
ATRIBUTOS EXTERNOS		
6	Administración	Capacidad de despliegue, instalación, actualización y monitoreo de software antivirus a través de la consola de administración. La administración centralizada no debe requerir un servidor dedicado. Configuración para formar grupos de

		equipos y aplicar distintas directivas y/o políticas del software antivirus por grupo de equipos a través de la consola de administración.
7	-Control web, Control de Inicio de Aplicación, Control de dispositivos	La solución debe tener un paquete de control web en cual pueda bloquear paginas web en su totalidad, grupo, individual además debe contar con un módulo que pueda bloquear paginas web por un horario determinado por el área de sistemas. El control de inicio de aplicaciones debe poder bloquear cualquier software de terceros ya sea de ejecución local o esté siendo ejecutado a través de un USB o CD- ROM determinado por el usuario. Debe poder bloquear cualquier aplicación que se ejecute automáticamente al insertar un USB o CD-ROM. La solución debe proporcionar un control centralizado de los dispositivos por bus, tipo de dispositivo o número de serie. Los administradores pueden aplicar un control detallado y aplicar políticas de uso adecuadas para los dispositivos de alto riesgo y asi, prevenir la transferencia de archivos potencialmente maliciosos a traves de un dispositivo y reducir el riesgo de fuga de dato.
8	Seguridad y Defensa contra Virus: Virus, Virus Troyanos, Macro Virus, Virus Gusano, Malware (Spyware, Adware),rootkits, Virus en archivos comprimidos.	El software antivirus debe ser capaz de proteger contra los programas malignos especificados.
9	Defensa en los Servidores de Red	Se requiere una solución basada en software. Deberá rastrear, eliminar virus y códigos maliciosos en los protocolos SMTP, HTTP y FTP. Deberá de poseer actualizaciones de patrones de búsqueda de virus de manera incremental, desatendida y automática. Protocolo SMTP Deberá tener capacidad de Relay de Correo Electrónico. Deberá tener capacidad de integración con el protocolo LDAP. Deberá de poder detectar y eliminar virus en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje. Deberá de realizar el bloqueo de archivos adjuntos de acuerdo a la extensión. Deberá de realizar el bloqueo de emails

		por asunto, destinatario o texto en el cuerpo del mensaje. Deberá de elegir distintas políticas para filtrar el contenido del tráfico entrante y del saliente. Deberá de poder hacer reglas de filtrado por usuarios. Deberá de poder hacer creaciones de listas de aceptación y negación (blancas y negras) de dominios y usuarios (cuentas de correo) confiables. Deberá de enviar notificaciones configurables al emisor, receptor y al administrador sobre mensajes electrónicos infectados. Deberá de contar con un administrador de cuarentena a nivel de consola. Protocolo FTP Deberá de ser capaz de revisar virus en las comunicaciones que se efectúen hacia los servidores FTP en tiempo real. Protocolo HTTP Deberá de revisar virus en las comunicaciones que se efectúen por medio de los navegadores web. Deberá de revisar y bloquear códigos maliciosos de Internet. Deberá de tener un filtro de URL's de páginas Web. Deberá de permitir de hacer reglas de restricción de navegación basado en el nombre de host, IP, usuarios y/o grupos.
10	Escaneo	Permitirá configurar la detección sobre todos los archivos, o tipos de archivos, comprimidos (cualquier formato de comprensión: rar, zip, cab, arj, arz), ocultos y archivos en ejecución. Deberá realizar los siguientes tipos de rastreo: en tiempo real, bajo demanda, programado y remoto a través de la consola de administración.
ATRIBUTOS DE USO		
12	Facilidad de Uso	El Software Antivirus debe incluir capacitación a usuarios para su uso más fácil y rápido.
13	Soporte Técnico a Usuarios	Debe ser 24x7x365
14	Eficacia	Debe ser capaz de permitir a los usuarios lograr las metas especificadas con exactitud e integridad, de acuerdo a sus especificaciones técnicas.
15	Integración con la Nube	La solución ofertada debe proporcionar protección basada en la nube de las nuevas amenazas identificadas por una comunidad de usuarios. La Solución deberá contar con un sistema de detección urgente (UDS)

		proporciona una rápida identificación de los archivos maliciosos y las URL que aprovechan los datos prácticos la nube para cambiar el tiempo de respuesta de seguridad de horas a segundos.
16	Productividad	No deberá consumir muchos recursos de memoria y procesador de los equipos usuarios.
17	Consideración como líder en el cuadrante Gartner	El software deberá ser considerado como líder en el cuadrante Garnert

e. **Establece Niveles, Escalas para las Métricas.**

ITEM	ATRIBUTOS	ESCALA
ATRIBUTOS INTERNOS		
1	Sistemas Operativos Estaciones de Trabajo	4
2	Sistemas Operativos Servidores de Red	4
3	Actualizaciones	6
4	Compatibilidad	6
5	Instalación	3
ATRIBUTOS EXTERNOS		
6	Administración	6
7	Control Web,aplicaciones,dispositivos	7
8	Seguridad y Defensa contra Virus	8
9	Defensa en los Servidores de Red	8
10	Escaneo	7
ATRIBUTOS DE USO		
11	Alertas y Reportes	8
12	Facilidad de uso	4
13	Soporte Técnico a Usuarios	5
14	Eficacia	8
15	Integración con la nube	6
16	Productividad	6
17	Consideración como líder en el cuadrante gartner	4
PUNTAJE TOTAL		100

V°B° OFICINA DE ESTADISTICA E INFORMATICA TZJ

f. **Criterios de Evaluación y Puntajes**

ITEM	ATRIBUTOS	ESET ENDPOINT SECURITY	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT	GDATA ENDPOINT PROTECTION BUSINESS	THE HACKER
ATRIBUTOS INTERNOS					
1	Sistemas Operativos Estaciones de Trabajo	4	4	2	3
2	Sistemas Operativos Servidores de Red	4	4	4	4
3	Actualizaciones	6	6	6	5
4	Compatibilidad	5	6	4	5
5	Instalación	1	3	1	1
ATRIBUTOS EXTERNOS					
6	Administración	5	6	6	5
7	Control Web, aplicaciones, dispositivos	3	7	5	4

8	Seguridad y Defensa contra Virus	7	8	7	6
9	Defensa en los Servidores de Red	8	8	8	7
10	Escaneo	7	7	7	6
ATRIBUTOS DE USO					
11	Alertas y Reportes	6	8	6	6
12	Facilidad de uso	4	4	3	4
13	Soporte Técnico a Usuarios	5	5	5	4
14	Eficacia	7	7	6	5
15	Integración con la nube	4	6	4	4
16	Productividad	6	6	6	5
17	Consideración como líder en el cuadrante Gartner	0	4	0	0
PUNTAJE TOTAL		77	99	80	74

En resumen tenemos:

SOFTWARE ANTIVIRUS	PUNTAJE TECNICO
ESET ENDPOINT SECURITY	77
KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT	99
GDATA ENDPOINT PROTECTION BUSINESS	80
THE HACKER	74

8. Conclusiones:

Adquirir el Antivirus KARSPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT, requiriéndose lo siguiente:

224	Licencia de Antivirus para Estaciones de Trabajo con sistema operativo Windows 8, Windows 7, Windows Vista, XP + Consola .
01	Licencia de Antivirus de correos Exchange 2010, 2008,2003,2000 (85 casillas de correo).
10	Licencia de Antivirus para Servidores para Windows Server 2012, 2008,2003,2000.

9. Firmas:

MINISTERIO DE SALUD
Hospital de Emergencias Pediátricas
Oficina de Estadística e Informática
Lic. TEODORO ZUASNABAR JUNES
COESPE N° 901

Lic. Teodoro Zuasnábar Junes
Director de Oficina de Estadística e Informática

MINISTERIO DE SALUD
Hospital de Emergencias Pediátricas
Oficina de Estadística e Informática
DIANA LIDIA REQUENA CAMPOVERDE

Sra. Diana L. Requena Campoverde
Responsable de Equipo de Trabajo de Informática