

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 1 de 10</b>



## **INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE**

**NÚMERO: P001-2013-GSTI**

**“ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS”**

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 2 de 10</b>

**1. NOMBRE DEL ÁREA:**

Gerencia de Sistemas y Tecnologías de la Información

**2. RESPONSABLES DE LA EVALUACIÓN:**

Javier Vilchez

**3. CARGOS:**

Coordinador de Soporte

**4. FECHA:**

Martes 08 de enero del 2013

**5. JUSTIFICACIÓN:**

La Municipalidad de Miraflores, a través de la Gerencia de Sistemas y Tecnología de la Información, cuya parte de sus funciones es velar por el normal funcionamiento en el ámbito informático y asesorar técnicamente en materia de adquisición de software y cumpliendo con la **RESOLUCIÓN MINISTERIAL N° 246-2007-PCM**, Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición” en todas las entidades integrantes del Sistema Nacional de Informática. Esta Norma Técnica Peruana establece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización.

Este informe tiene como propósito, analizar las alternativas para implementar la solución que garantice identificar los peligros de este tipo de riesgo, lo cual ayudará a tomar acciones antes que las amenazas informáticas impacte negativamente en los recursos (activos) de la infraestructura de nuestra red. Así mismo se requiere que la solución permita implementar el Control de Acceso a la Red (NAC) en todas las áreas de la institución para comprobar que todos los equipos que acceden a la red, incluso los que no pertenecen a la empresa, cumplan las normativas y políticas de seguridad.

La Municipalidad de Miraflores viene usando desde el 2012 el software de antivirus Sophos para la protección y seguridad de la información tanto para equipos de escritorio, portátiles y/o servidores.

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 3 de 10</b>

Por protección Anti-Virus, se entiende como una solución brindada por un conjunto de herramientas que garanticen la seguridad y el control sobre cualquier tipo de software malintencionado como virus informáticos, incluidos:

Por las razones expuestas la Municipalidad de Miraflores necesita contar con un Software Antivirus que brinde la protección, seguridad y estabilidad a la información institucional las cuales se almacenan en las estaciones de trabajo, ordenadores portátiles y servidores tanto para servidores con equipos windows como Open source (Linux).

Cabe mencionar que las Licencias actuales tienen vigencia hasta el 05 de Marzo del 2013 por lo que es necesario que las licencias del nuevo producto antivirus tenga vigencia a partir del día siguiente a fin de evitar problemas con la legalidad del software.

## 6. ALTERNATIVAS:

Considerando los requerimientos de la Municipalidad de Miraflores se ha buscado, y comparado alternativas de software de antivirus en el mercado nacional los cuales deben de cumplir con los requerimientos suficientes para mantener y/o mejorar la seguridad y protección de la información de los equipos finales en la Municipalidad de Miraflores.

Los productos a evaluar considerando un licenciamiento para un mínimo de 550 dispositivos de la Municipalidad son:

- ✦ BitDefender Small Office Security
- ✦ Kaspersky Security Edition
- ✦ Avira Endpoint Security
- ✦ Sophos Endpoint Security

Los software fueron evaluados con sistemas operativos Microsoft Windows xp, Windows 7 *(Se indica además que una vez determinado el software Antivirus en este se consideran también equipos con distribución Windows tanto para Windows Server 2003, Windows Server 2008, Windows Server 2012, así como las distribuciones para servidores y equipos Linux).*

## 7. ANALISIS COMPARTIDO TECNICO

### ✦ Propósito de evaluación

Validar que las alternativas seleccionadas sean las mas convenientes para la Municipalidad de Miraflores.

### ✦ Identificar el tipo de producto

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 4 de 10</b>

Software de antivirus corporativo para estaciones de trabajo y servidores.

#### ⤴ **Especificaciones del modelo de calidad**

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM

#### ⤴ **Selección de métricas**

Las métricas fueron seleccionadas en base al análisis de la información técnica de los productos antivirus señalados en el punto "6. ALTERNATIVAS", como son las características del Producto y requerimientos de instalación de las empresas proveedoras siendo estas:

- ⤴ IT Global
- ⤴ Tech Mind Solutions
- ⤴ Labset Protec
- ⤴ Innovare

Del análisis realizado se ha determinado las siguientes características técnicas mínimas:

ITEM	ATRIBUTOS	DESCRIPCIÓN
<b>ATRIBUTOS INTERNOS</b>		
1	Sistemas Operativos Estaciones de Trabajo	<ul style="list-style-type: none"> <li>⤴ Windows XP/Vista/7/32/64 bits, Mac OS X Tiger (10.4.6 o posterior), Mac OS X Leopard (10.5 o posterior), Mac OS X Snow Leopard (10.6 o posterior)</li> <li>⤴ Red Hat Linux, Opensuse Linux, Ubuntu Linux</li> <li>⤴ La solución deberá soportar las versiones de 32 y 64bits.</li> </ul>
2	Sistemas Operativos Servidores de Red	<ul style="list-style-type: none"> <li>⤴ Microsoft Windows Server 2003 32/64 bits, Windows 2008, Windows Server 2012</li> <li>⤴ Red Hat Enterprise Linux 5 Server, Red Hat Enterprise Linux 6 Server, OpenSuse Linux 11, Ubuntu Linux Server 12.04</li> <li>⤴ La solución deberá soportar las versiones de 32 y 64bits para las plataformas</li> </ul>

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 5 de 10</b>

		<p>descritas.</p>
3	Actualizaciones de firmas	<p>⤴ Deben ser 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.</p>
4	Protección Proactiva	<p>⤴ La solución debe contar con una tecnología de detección proactiva de amenazas conocidas y desconocidas que detecte malware “antes de su ejecución (pre-execution)” y “en ejecución (on-execution)”.</p>
5	Protección Contra la Pérdida de Información	<p>⤴ La solución debe contar con un sistema del mismo fabricante que permita controlar o bloquear el uso de dispositivos USB, Grabadores CD/DVD, Floppy Drives, Lectores CD/DVD, HDD Externos y dispositivos Wireless como Wi-Fi; mediante la creación y administración de políticas de Uso de Dispositivos, las cuales permitan cumplir con los requerimientos de seguridad de la información.</p>
6	Control y Productividad en la Red	<p>⤴ El sistema de control de aplicaciones y filtros debe ser mantenida por el fabricante y podrá opcionalmente actualizar categorías en forma automática. No se aceptarán soluciones que necesiten la intervención del administrador de la solución para mantener al día dichas categorías y/o listas de aplicaciones a controlar.</p> <p>⤴ El sistema deberá de contar con informes históricos de auditoria que permitan controlar la instalación de software no autorizado por la Institución.</p>
7	Compatibilidad	<p>⤴ Con los sistemas operativos en las versiones anteriores mencionadas.</p>
8	Instalación	<p>⤴ La instalación del software a las computadoras de los usuarios debe ser mediante:</p> <ul style="list-style-type: none"> <li>◦ Sincronización con el Directorio Activo de Microsoft o Servidor de</li> </ul>

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 6 de 10</b>

		<p>Autenticación en Linux</p> <ul style="list-style-type: none"> <li>◦ La Consola de Administración e Instalación mediante CD o recurso UNC (formato de dirección para especificar la ubicación del recurso)</li> </ul>
<b>ATRIBUTOS EXTERNOS</b>		
9	Consola de Administración	<p>⤴ La herramienta debe contar con una Consola de Administración desde donde se pueda Administrar y controlar la solución antivirus en forma centralizada. Con posibilidad de integrar gestión y administración en la nube.</p>
10	Protección y Defensa frente a malware en Estaciones y Servidores	<p>⤴ La solución de seguridad para estaciones y servidores debe ser de tipo Integrada; es decir debe incluir un único agente que brinde protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, detección web de ataques de scripts maliciosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red.</p>
11	Escaneo	<p>⤴ Permitir 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. En tiempo real, bajo demanda, programado y remoto a través de la consola de administración.</p>
12	Productividad	<p>⤴ No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.</p>
<b>ATRIBUTOS DE USO</b>		
13	Alertas y Reportes	<p>⤴ La consola de administración deberá de ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.) Generar reportes gráficos imprimibles y exportables de la cobertura de versiones,</p>

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 7 de 10</b>

		actualizaciones e infecciones.
14	Facilidad de Uso	⤴ Toda la solución deberá incluir capacitación a usuarios para el uso más fácil y rápido.
15	Seguridad del Producto	⤴ El producto debe contar con medidas de seguridad para que el usuario de la estación de trabajo no deje sin efecto políticas corporativas a la vez que está integrado con el agente NAC de la solución:
16	Proveedor	⤴ Debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. El postor deberá presentar un documento del fabricante donde certifique que cuenta con este tipo de soporte.
17	Eficacia	⤴ Deberá ser capaz de permitir al área de TI de la entidad lograr las metas específicas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimiento de la organización.

⤴ **Niveles, escalas para las métricas**

ITEM	ATRIBUTOS	ESCALAS
<b>ATRIBUTOS INTERNOS</b>		
1	Sistemas Operativos Estaciones de Trabajo	5
2	Sistemas Operativos Servidores de Red	5
3	Actualizaciones de firmas	5
4	Protección Proactiva	7
5	Protección contra la Pérdida de Información	7
6	Control y Productividad en la red	7
7	Compatibilidad	5
8	Instalación	6
<b>ATRIBUTOS EXTERNOS</b>		

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración: 08/01/2013</b>
		<b>Página 8 de 10</b>

9	Consola de Administración	5
10	Protección y Defensa frente a malware en Estaciones y Servidores	6
11	Escaneo	5
12	Productividad	5
<b>ATRIBUTOS DE USO</b>		
13	Alertas y Reportes	6
14	Facilidad de uso	7
15	Seguridad del Producto	6
16	Proveedor	7
17	Eficacia	6
<b>PUNTAJE TOTAL</b>		<b>100</b>

### EVALUACION COMPARATIVA

Item	Atributos	Avira	Kaspersky	BitDefender	Sophos	Puntaje
<b>ATRIBUTOS INTERNOS</b>						
1	Sistemas Operativos Estaciones de Trabajo	4	5	5	4	5
2	Sistemas Operativos Servidores de Red	2	4	4	2	5
3	Actualizaciones de firmas	3	3	5	2	5
4	Protección Proactiva	3	5	7	3	7
5	Protección contra la Pérdida de Información	3	3	3	3	7
6	Control y Productividad en la red	3	5	7	2	7
7	Compatibilidad	3	5	5	2	5
8	Instalación	3	4	6	4	6
<b>ATRIBUTOS EXTERNOS</b>						
9	Consola de Administración	3	3	5	3	5

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 9 de 10</b>

10	Protección y Defensa frente a malware en Estaciones y Servidores	3	4	6	3	6
11	Escaneo	3	3	5	3	5
12	Productividad	3	4	5	2	5
<b>ATRIBUTOS DE USO</b>						
13	Alertas y Reportes	3	5	4	3	6
14	Facilidad de uso	5	5	7	5	7
15	Seguridad del Producto	2	4	6	3	6
16	Proveedor	6	6	6	5	7
17	Eficacia	6	6	6	3	6
	<b>Total</b>	<b>60</b>	<b>74</b>	<b>92</b>	<b>52</b>	<b>100</b>

## 8. ANALISIS COMPARATIVO DE COSTO – BENEFICIO

### 8.1 Costo

El presente documento tiene la finalidad de obtener las mejores características técnicas disponibles en el mercado para la solución que requiere la Municipalidad por lo que la obtención del costo no es materia del presente. Sin embargo, de acuerdo a los procedimientos administrativos la obtención del precio referencial será realizada previa a la convocatoria y corresponde al área responsable realizar el análisis de costo respectivo.

### 8.2 Beneficio

La adquisición de **SOFTWARE DE SOLUCIÓN ANTIVIRUS** permitirá:

- Proteger las pc de virus informáticos, malware, troyanos, gusanos. Que son programas maliciosos que pueden robar/borrar la información contenida en los discos duros del equipo y/o tomar el control de la pc para iniciar ataques informáticos a otros objetivos dentro o fuera de la red.
- Permite restricción en el uso de aplicaciones específicas como p.e. el uso de ares, desde la consola de antivirus se puede establecer políticas que impidan que los usuarios usen este tipo de aplicaciones.
- Proteger del acceso a páginas consideradas peligrosas, por contener código malicioso que podría tomar las credenciales ingresadas por los usuarios a través de las páginas web (tarjetas de crédito, contraseñas de correo, etc)

	<b>TIPO: INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	<b>Código: P001-2013-GSTI</b> <b>Versión: 1.0</b>
	<b>TITULO: ADQUISICION DE SOFTWARE DE SOLUCION DE ANTIVIRUS</b>	<b>Fecha de Elaboración:</b> <b>08/01/2013</b>
		<b>Página 10 de 10</b>

- La solución antivirus incluye la protección de pc de usuario y servidores.
- Permite restringir el uso de dispositivos de almacenamiento externo como usb para impedir que el usuario pueda inadvertidamente contagiar de virus su pc o para que no valla a llevarse información sensible.

## 9. CONCLUSIONES

- ⤴ La cantidad de Licencias del software de antivirus a adquirir para la Municipalidad de Miraflores es de 550 entre estaciones de trabajo y servidores esto incluye actualización de las versiones durante ese periodo.
- ⤴ El soporte técnico será tanto en sitio como remoto (vía teléfono o correo electrónico), en un tiempo de 24x7.
- ⤴ Soporte de plataforma tanto para equipos de 32 bit como de 64 bit.
- ⤴ El proveedor del producto elegido tiene que contar con un personal certificados por el fabricante del software en los bienes ofertados para brindar la garantía comercial requerida.
- ⤴ Se deberá de incluir una capacitación del producto como mínimo para 3 personas, para efectuar la administración debida.
- ⤴ La vigencia de las licencias seran por 1 año.
- ⤴ BitDefender Business Security, tuvo un mejor rendimiento y detección en cuanto a búsqueda de virus, malwares.
- ⤴ Kaspersky, presento opciones adicionales de reportes
- ⤴ Avira demostró lentitud y congelamiento en algunos equipos con windows, y además de una dificultad al momento de realizar la desinstalacion de este.
- ⤴ El sophos tiene algunas vulnerabilidades en cuando a malware, así como algunas debilidades en cuanto escaneo de los equipos.
- ⤴ Por ello como mejor alternativa se sugiere el software BitDefender, por las observaciones mencionadas y por el resultado del análisis para la Municipalidad de Miraflores.

## 10. FIRMAS

Responsable de la evaluación	Firma
Javier Vilchez López	