 Servicio de Administración Tributaria de Lima	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 25/10/2010
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 1 de 7

**INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N°030-2010-GIN/SAT**

**1. NOMBRE DEL ÁREA:**

Gerencia de Informática

**2. RESPONSABLES DE LA EVALUACIÓN:**

Cesar Terry Ramos

**3. CARGO:**

Jefe de División de Soporte y Producción.

**4. FECHA DE APROBACION**

25 de Octubre del 2010

**5. JUSTIFICACIÓN**

El Servicio de Administración Tributaria SAT Lima, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de la información importante de la institución, así como el normal desarrollo de sus funciones, la institución requiere contar con una Solución de Seguridad y Control de Acceso a la Red.

De acuerdo a Ley es necesario evaluar programas de software que cumplan con las especificaciones técnicas requeridas, a fin de proceder a su adquisición.

**6. ALTERNATIVAS.**

Se analizaron los siguientes productos:


- McAfee NAC
- Sophos NAC
- Symantec NAC

**7. ANALISIS COMPARATIVO TÉCNICO**

Se procedió en aplicación de la parte 3 de la Guía de Evaluación de Software aprobada por Resolución Ministerial N° 139-2004-PCM:

a. Propósito de la Evaluación:

- Determinar los atributos o características mínimas para el Producto Final.

	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 25/10/2010
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 2 de 7


- b. Identificar el tipo de producto
- Software para Seguridad y Control de Acceso a la Red.
- c. Especificaciones del Modelo de Calidad
- Se aplica al Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial No 139-2004-PCM.
- d. Selección de Métricas
- Las métricas fueron seleccionadas en base al análisis de los requerimientos del área usuaria y a la información técnica de los productos de Software señalados en el punto "6. ALTERNATIVAS"

Del análisis realizado, se han determinado las siguientes características técnicas mínimas y sus respectivas métricas.

ITEM	CARACTERISTICAS	DESCRIPCION
<b>ATRIBUTOS INTERNOS</b>		
1	Sistemas operativos de estaciones de trabajo	<p>Se podrá instalar en los equipos de la red una versión pre-configurada del agente.</p> <p>El sistema debe prever el Acceso de equipos no administrados (proveedores, invitados, etc.) mediante un agente soluble (agente que no se requiere ser instalado para ejecutar las tareas de control de acceso a la red)</p> <p>Ambos métodos deberán soportar multiplataforma como:</p> <ul style="list-style-type: none"> <li>▪ Microsoft Windows 2000, XP, Vista y 7.</li> </ul> <p>Utilizando un agente instalado en el usuario los siguientes sistemas y navegadores deben ser soportados:</p> <ul style="list-style-type: none"> <li>▪ Windows 7: Cualquier versión, SP y Internet Explorer</li> <li>▪ Windows Vista: cualquier versión, SP y Internet Explorer</li> <li>▪ Windows XP: cualquier versión, SP y Internet Explorer</li> <li>▪ Windows 2000: , cualquier versión, SP y Internet Explorer</li> </ul>
2	Soporte de Autenticación	<p>Debe permitir la autenticación de los usuarios y la estación de trabajo antes de presentar las credenciales y luego de haber ingresado los datos del usuario.</p> <p>La autenticación por maquina permitirá la remediación automática sin intervención del usuario.</p> <p>La autenticación de los usuarios podrá estar integrada con la autenticación en el dominio Windows.</p> <p>Debe permitir asignar uno o más grupo/s al usuario dependiendo de cualquier atributo, especificado por el administrador, obtenido de su fuente de autenticación (por ejemplo LDAP, Radius).</p> <p>Deberá soportar la autenticación para equipos de red como:</p>

		<ul style="list-style-type: none"> <li>▪ Alcatel, Aruba Networks, Aventail, Cisco, Checkpoint, Juniper Networks, 3COM, Nortel, Novel, Lucent.</li> </ul> <p>Deberá integrarse con varios mecanismos de autenticación como Directorio Activo, DHCP, LDAP, RADIUS, 802.1 y Portal Web.</p> <p>Deberá contar con agentes persistentes (instalados en clientes) y en modo web (solubles).</p>
3	Actualizaciones	<p>El Sistema debe almacenar los logs de todos los pedidos de autenticación de los usuarios como también los resultados de cumplimiento de normas de cada uno de ellos.</p> <p>Debe poder almacenar al menos:</p> <ul style="list-style-type: none"> <li>▪ Información del usuario que se registra (log in) y del que finalice su sesión (log-out).</li> <li>▪ Timeout de sesiones, incluyendo tiempos sin actividad y tiempos máximos de sesión.</li> <li>▪ Cumplimiento de las políticas de seguridad y auditoria por usuario.</li> <li>▪ Estado de las comunicaciones entre los Agentes y la consola de administración.</li> <li>▪ Cantidad de usuarios que ingresan al sistema con/sin éxito.</li> </ul> <p>Debe permitir el acceso en tiempo real a los reportes y análisis de la seguridad en la red.</p> <p>Los reportes no deben estar limitados a los principales incidentes sino a todas pudiendo para ello crear filtros personalizados.</p>
<b>ATRIBUTOS EXTERNOS</b>		
4	Configuración	<p>El Administrador de Políticas debe permitir generar roles de administración por atributos.</p> <p>Los administradores deben contar con perfiles de acceso con lectura/escritura o solo lectura para cada una de las funciones de configuración: configuración, gestión, roles, tareas administrativas, tareas de mantenimiento, entre otras.</p> <p>La configuración del equipo debe poder ser guardada y/o exportada en forma programada a un repositorio de configuraciones externo.</p>
5	Gestión y Monitoreo	<p>La solución deberá contar con un administrador Web Seguro (SSL).</p> <p>Reportes de la consola de administración:</p> <ul style="list-style-type: none"> <li>▪ Equipos que cumplen con las políticas</li> <li>▪ Equipos que no cumplen con las políticas</li> <li>▪ Equipos que parcialmente cumplen con las políticas.</li> <li>▪ Detalle completo del cumplimiento de la seguridad para: <ul style="list-style-type: none"> <li>○ Anti-virus, Firewall, Parches, Encriptamiento, Anti-Spyware, Aplicaciones personalizadas.</li> </ul> </li> </ul> <p>La solución deberá evaluar el cumplimiento en tiempo real, es decir, no deberá requerirse ejecutar reportes para conocer el estado de cumplimiento de la seguridad en la red.</p>

6	Control de Acceso	<p>Debe poseer un modelo de políticas de seguridad basada en roles.</p> <p>Debe permitir asignar recursos a los usuarios dependiendo del nivel de autorización, incluyendo control granular sobre URL permitidos.</p> <p>Debe permitir aplicar políticas para usuarios o grupos específicos a fin de garantizar que el acceso a la información, los servidores y las aplicaciones solamente estén disponibles para aquellos equipos que están autorizadas.</p> <p>Debe bloquear aplicaciones no deseadas con la finalidad de prevenir la fuga de datos en la organización.</p> <p>Debe permitir garantizar que la función de Control de Fuga de Datos y Control de dispositivos que posee la institución esté activada.</p> <p>Deberá integrarse con varios mecanismos de autenticación como Directorio Activo, DHCP, LDAP, RADIUS, 802.1, Portal Web y autenticación VPN.</p>
<b>ATRIBUTOS DE USO</b>		
7	Seguridad Multiplataforma	<p>Capacidad de poder ser integrado con equipos de seguridad que complemente su capacidad para brindar restricciones avanzadas de seguridad frente a diversos ataques.</p> <p>Permitir una respuesta automática para aislar, deshabilitar o tomar alguna restricción al usuario que sea identificado como atacante.</p> <p>En el caso de contar con múltiples dispositivos de seguridad, permitir la administración mediante una consola centralizada, independiente de la consola de administración del equipo.</p> <p>Niveles dinámicos de seguridad capa 2, mediante la autenticación 802.1X.</p> <p>Permitir la integración con conmutadores y puntos de acceso inalámbrico que soporten esta tecnología.</p> <p>Debe integrarse con las aplicaciones de seguridad y la infraestructura de red existente sin requerir cambios en ellas.</p>
8	Reporte, Remediación y Reforzamiento	<p>Debe soportar la generación de reportes dinámicos dependiendo del grado de seguridad de la estación de trabajo.</p> <p>Debe permitir evaluar los equipos antes del acceso a la red o durante la sesión.</p> <p>Debe poseer las siguientes funcionalidades de verificación:</p> <ul style="list-style-type: none"> <li>▪ Verificación de versiones y aplicaciones "aceptadas".</li> <li>▪ Verificación de antivirus instalado y operativo.</li> <li>▪ Verificación firewall personal instalado y operativo.</li> </ul> <p>La verificación mencionada anteriormente debe contemplar reglas pre-establecidas de las siguientes categorías de productos que pueden potencialmente estar instalados en un puesto de trabajo:</p> <ul style="list-style-type: none"> <li>▪ Antivirus: Authentium, BitDefender, AVG, Clamwin, CA, Dr</li> </ul>

 Servicio de Administración Tributaria de Lima	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 25/10/2010
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 5 de 7

		<p>Web, Symantec (Norton), McAfee, Panda, Sophos, F-Secure, Kaspersky Labs, Zone Labs, SBC Yahoo AV, Trend Micro, Antivir, F-Prot, Nod 32, Sophos.</p> <ul style="list-style-type: none"> <li>▪ Firewall: ISS, Microsoft, Symantec (Norton and Sygate), McAfee, Zone Labs, Tiny Software (CA), etc.</li> <li>▪ Spyware: Lavasoft (Ad-aware), Computer Associates (Pest Patrol), McAfee, Prevx, Webroot (spy sweeper), PCTools (spyware doctor), Java cool software (spyware blaster), Microsoft, Trend Micro, Bulletproofsoft, Spyware begone, SBC Yahoo.</li> </ul> <p>Debe garantizar que la seguridad en los equipos esté actualizada verificando contra una base de datos de parches (al menos 600 parches de seguridad predefinidos) y aplicaciones de seguridad (al menos 500 predefinidas).</p> <p>El sistema debe prever el Acceso de equipos no administrados (proveedores, invitados, etc.) mediante un agente no-instalable y que se ejecute en forma automática al momento de conectarse a la red.</p> <p>No deberá requerirse privilegios de administrador para la verificación de políticas.</p> <p>Deberá soportar la auto-remediación.</p> <p>Deberá soportar la creación de políticas personalizadas para aplicaciones que la entidad lo determine.</p> <p>Deberá soportar la capacidad de reforzamiento mediante DHCP, 802.1x, Cisco NAC y VPN e IPsec.</p> <p>Deberá soportar la capacidad de reforzamiento en los siguientes niveles de estaciones, L2 Lan Switch, Router / L3 LAN Switch, SSL VPN Gateway y Puntos de Acceso Wireless.</p>
9	Soporte técnico	Existe Distribuidor oficial que brinde el soporte técnico de primera línea en la modalidad de 24/7.

e. Niveles, escalas para las métricas.

ITEM	ATRIBUTOS	Puntaje Máximo
<b>ATRIBUTOS INTERNOS</b>		
1	Sistemas operativos de estaciones de trabajo	10
2	Soporte de Autenticación	10
3	Actualizaciones	10
<b>ATRIBUTOS EXTERNOS</b>		
4	Configuración	10
5	Gestión y Monitoreo	12

 Servicio de Administración Tributaria de Lima	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 25/10/2010
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 6 de 7

6	Control de Acceso	12
<b>ATRIBUTOS DE USO</b>		
7	Seguridad Multiplataforma	12
8	Reporte, Remediación y Reforzamiento	12
9	Soporte técnico	12
<b>TOTAL</b>		<b>100</b>

Determinar las características técnicas mínimas y las métricas aplicables, se procedió al análisis comparativo técnico, para lo cual se aplicó el Modelo de Calidad de Software descrito en la Parte I de la Guía Evaluación de Software por Resolución Ministerial No 139-2004-PCM.

ITEM	ATRIBUTOS	McAfee	Sophos	Symantec	Puntaje Máximo
<b>ATRIBUTOS INTERNOS</b>					
1	Sistemas Operativos Estaciones de Trabajo	10	10	10	10
2	Soporte de Autenticación	10	10	10	10
3	Actualizaciones	9	10	9	10
<b>ATRIBUTOS EXTERNOS</b>					
4	Configuración	10	10	10	10
5	Gestión y Monitoreo	11	12	11	12
6	Control de Acceso	11	11	11	12
<b>ATRIBUTOS DE USO</b>					
7	Seguridad Multiplataforma	12	12	12	12
8	Reporte, Remediación y Reforzamiento	11	12	11	12
9	Soporte técnico	12	12	12	12
<b>TOTAL</b>		<b>96</b>	<b>99</b>	<b>96</b>	<b>100</b>

## 8. ANALISIS COMPARATIVO DE COSTO - BENEFICIO

### Licenciamiento:

Se requiere la adquisición de seis cientos (600) licencias de software NAC, para aportar en la Solución de Seguridad y Control de Acceso a la Red.

### Mantenimiento:

La adquisición de las licencias de software, debe considerar la suscripción anual de soporte y mantenimiento.

Se ha realizado el análisis comparativo de costos de los productos señalados en el punto 6: ALTERNATIVAS.

Producto	Nro Licencias	Total S/	Observaciones
McAfee	600	63,000.00	Adquisición Nueva
Sophos	600	45,000.00	Adquisición Nueva
Symantec	600	74,400.00	Adquisición Nueva

 SAT Servicio de Administración Tributaria de Lima	<b>LEY 28612</b> LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 25/10/2010
	<b>INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE</b>	Página 7 de 7

**Hardware:**

Todos productos se adaptan y son compatibles con la plataforma informática de Hardware.

**Beneficios:**

Los Beneficios obtenidos a partir de la implementación del uso del software, sobre la plataforma de equipos informáticos, han sido entre otros:

- EI SISTEMA DE CONTROL DE ACCESO A REDES LAN permitirá el control de acceso a la red de la SAT en forma segura y mediante la validación de políticas de seguridad en los equipos de la red.

**9. CONCLUSIONES**

Se determinaron los atributos o características técnicas que deben ser consideradas en la evaluación del software, estableciéndose la valoración de cada característica dentro del modelo descrito en la Parte de la Guía de Evaluación de Software aprobado por resolución Ministerial No 139-2004-PCM.

De acuerdo a los trámites comparativos técnicos y de recursos económicos de todo el sistema actual para la Solución de Seguridad y Control de Acceso a la Red, se ha podido determinar que el software de la firma Sophos, Producto: Sophos NAC Advanced, cumple como la mejor alternativa. Sin embargo se deberá realizarse un proceso de selección si es que administrativamente lo amerita.

**10. FIRMAS**

  
**CESAR TERRY RAMOS**  
Jefe de Soporte y Producción  
Servicio de Administración Tributaria