ZOFRATACNA
ZONA FRANCA DE TACNA - PERU

INFORME TÉCNICO PREVIO DE EVALUACION DE SOFTWARE N° 001-2010-GS-ATI

"LICENCIAMIENTO DEL SOFTWARE ANTI-VIRUS"

1. **NOMBRE DEL ÁREA:**
   Gerencia de Servicios - Área de Tecnologias de la Información

2. **RESPONSABLES DE LA EVALUACION:**
   Ing. Ivan Rojas Morales

3. **CARGOS:**
   Asistente en Soporte y Software.

4. **FECHA:**
   24 de Setiembre de 2010

5. **JUSTIFICACION:**
   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.

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

   1. Macros;
   2. Software espía (spyware) y/o malware en general;
   3. Generadores de correo basura y elementos de software diseñados para la obtención, robo y utilización no autorizada de información critica, así como para el re-enrutamiento de solicitudes de servicio hacia servidores no autorizados y/o suplantando a los originales, situaciones conocidas bajo los términos de phishing y pharming en los siguientes niveles:

      a) Protección de Estaciones y Servidores:
         - Anti-Virus / Anti-Rootkit, Anti-Adware / Anti-Spyware / Anti-Malware,
         - Detector de Intrusos de Host,

- Control de Aplicaciones y Dispositivos,
- Control de Acceso a la Red.

b) Protección en el Servidor de Correo:
- Anti-virus / Anti-Spyware / Anti-Adware,
- Control y Filtrado del Contenido de Correo.

6. ALTERNATIVAS:

Se analizaron los siguientes productos antivirus:

- **Antivirus Nacionales:** PER, The Hacker.
- **Antivirus Extranjeros:** Panda, Eset Nod32, Bitdefender y Sophos.

7. ANALISIS COMPARATIVO TÉCNICO:

Característica Técnica	Antivirus Nacionales	Antivirus Extranjeros
Soporte de las siguientes plataformas operativas de estaciones de trabajo: Windows 2000, Windows XP, Windows Vista, Windows 7.	Si soportan las plataformas solicitadas.	Si soportan las plataformas solicitadas.
Soporte las siguientes plataformas operativas de servidores: Windows 2000/2003 Server y Linux.	Si soportan las plataformas solicitadas.	Si soportan las plataformas solicitadas.
Tiene un módulo residente, ejecutándose en la memoria del sistema, comúnmente llamado scanner "on-access" y un modulo de revisión antivirus ejecutado en forma manual por el usuario, comúnmente llamado scanner "on-demand".	Si lo tienen.	Si lo tienen.
Soporte nativo del MTA (Mail Transport Agent) del servidor de correos Linux: Postfix.	No disponen.	Si disponen.
Certificación de Red Hat para el antivirus del servidor de correos Linux.	No disponen.	Solo algunos fabricantes tienen dicha certificación.
Detección de spyware y adware en las estaciones de trabajo.	Si disponen.	Si disponen.
La consola de administración no requiere servidor dedicado.	Si disponen.	Solo algunos fabricantes disponen esta caracteristica.
Actualización de firmas de virus de manera incremental, automática y desatendida.	No dispone.	Si disponen.
Cuenta con una plataforma NAC (Network Access Control) incluida en la solución.	No disponen.	Solo algunos productos disponen estas caracteristicas.

Se realizó aplicando la parte 3 de la Guia de Evaluación de Software:

a. Propósito de la Evaluación:

- Determinar los atributos o caracteristicas minimas para el Producto Final Software requerido.

b. Identifica el tipo de producto:

- Software de Seguridad Antivirus Servidor Cliente.

c. Especificación del Modelo de Calidad:

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

d. 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 Caracteristicas del Producto y Requerimientos de instalación

  Del análisis realizado se ha determinado las siguientes caracteristicas técnicas minimas:

ITEM	ATRIBUTOS	DESCRIPCIÓN
ATRIBUTOS INTERNOS		
01	Sistemas Operativos Estaciones de Trabajo.	✓ Windows 98/2000/XP/Vista/7 ✓ La solución deberá soportar las versiones de 32 y 64 bits.
02	Sistemas Operativos Servidores de Red	✓ Microsoft Windows 2000 Server, Microsoft Windows Server 2003, Windows Server 2008 ✓ Red Hat Enterprise Linux 5 Server, ✓ La solución deberá soportar las versiones de 32 y 64 bits para las plataformas descritas.
03	Actualizaciones de firmas	✓ 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.
04	Protección Proactiva	✓ 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)".
05	Protección Contra la Pérdida de Información	✓ 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.
06	Control y Productividad en la Red	✓ El sistema de control de aplicaciones debe ser mantenida por el fabricante y deberá actualizar las 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.
07	Compatibilidad	✓ Con los sistemas operativos en las versiones anteriores mencionadas.
08	Instalación	✓ La instalación del software a las computadoras de los usuarios debe ser mediante: ○ Sincronización con el Directorio Activo de Microsoft o Servidor de Autenticación en Linux ○ La Consola de Administración e ○ Instalación mediante CD o recurso UNC (formato de dirección para especificar la ubicación del recurso).
ATRIBUTOS EXTERNOS		
09	Consola de Administración.	✓ La herramienta debe contar con una Consola de Administración desde donde se pueda Administrar y controlar la solución antivirus en forma centralizada.
10	Protección y Defensa frente a malware en Estaciones y Servidores	✓ 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.
11	Escaneo	✓ 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.
12	Productividad	✓ No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.
13	Protección en el Servidor de Correo (Protocolo SMTP)	✓ Se requiere una solución del mismo fabricante que brinde Seguridad y Control de la información entrante y saliente de la red vía los protocolos SMTP el cual deberá incluir su propio motor MTA.

ATRIBUTOS DE USO		
14	Alertas y Reportes	✓ 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, actualizaciones e infecciones.
15	Facilidad de Uso	✓ Toda la solución deberá incluir capacitación a usuarios para el uso más fácil y rápido.
16	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
17	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.
18	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.

e. **Niveles, escalas para las Métricas:**

ITEM	ATRIBUTOS	ESCALAS
	ATRIBUTOS INTERNOS	
01	Sistemas Operativos Estaciones de Trabajo	5
02	Sistemas Operativos Servidores de Red	5
03	Actualizaciones de firmas	5
04	Protección Proactiva	7
05	Protección contra la Pérdida de Información	7
06	Control y Productividad en la Red	7
07	Compatibilidad	5
08	Instalación	4
	ATRIBUTOS EXTERNOS	
09	Consola de Administración	5
10	Protección y Defensa frente a malware en Estaciones y Servidores	6
11	Escaneo	4
12	Productividad	4
13	Protección en el Servidor de Correo	6
	ATRIBUTOS DE USO	
14	Alertas y Reportes	6
15	Facilidad de uso	5
16	Seguridad del Producto	6
17	Proveedor	7
18	Eficacia	6
	PUNTAJE TOTAL	100

No se ha comparado los productos de software antivirus, porque el objetivo del presente documento es establecer características técnicas mínimas de la solución antivirus.

ITEM	ATRIBUTOS	Antivirus Nacionales	Antivirus Extranjeros	Puntaje Máximo
	ATRIBUTOS INTERNOS			
01	Sistemas Operativos Estaciones de Trabajo	4	5	5
02	Sistemas Operativos Servidores de Red	4	5	5
03	Actualizaciones de firmas	5	5	5
04	Protección Proactiva	6	7	7
05	Protección contra la Pérdida de Información	2	6	7
06	Control y Productividad en la Red	2	6	7
07	Compatibilidad	5	5	5
08	Instalación	4	4	4
	ATRIBUTOS EXTERNOS			
09	Consola de Administración	3	5	5
10	Protección y Defensa frente a malware en Estaciones y Servidores	6	6	6
11	Escaneo	4	4	4
12	Productividad	4	4	4
13	Protección en el Servidor de Correo	3	6	6
	ATRIBUTOS DE USO			
14	Alertas y Reportes	5	6	6
15	Facilidad de uso	5	5	5
16	Seguridad del Producto	6	6	6
17	Proveedor	7	5	7
18	Eficacia	6	6	6
	TOTAL	**76**	**96**	**100**

8. ANALISIS COMPARATIVO DE COSTO – BENEFICIO:

Diariamente a nivel mundial aparecen más de 20 nuevos virus, y en el mundo globalizado, que se vive actualmente, esto es una amenaza constante para cualquier institución, por ello es necesario contar con un software de antivirus que cubra todos los puntos de red: estaciones, servidores, oficinas remotas, dispositivos móviles de ZOFRATACNA.

- **Licenciamiento.**

  La solución deberá de incluir licencias antivirus con mantenimiento de software (cambios de versión, actualización y firmas de virus) por 01 año.

De igual forma, la solución incluirá la actualización permanente de las herramientas y elementos que componen la solución, en términos de listas y definiciones de virus, así como de la lógica (motores de revisión – engines), tecnologías y técnicas utilizadas por el fabricante de la solución EN TODOS y CADA UNO de los componentes que la constituyen.

Todos los productos ofrecidos DEBEN corresponder a las últimas versiones.

- **Hardware necesario para su funcionamiento.**

La solución antivirus se instalará en toda la infraestructura existente de ZOFRATACNA, tales como estaciones de trabajo, servidores de archivos y/o aplicaciones, servidores de base de datos y en los servidores de correo.

- **Soporte y mantenimiento externo.**

El fabricante de los productos ofertados DEBE poseer oficina de representación en Perú, en la Zona Sur (Arequipa, Moquegua, Tacna) y/o tener la categoría de representante oficial, así como personal de soporte técnico que garantice la adecuada y oportuna prestación de la garantía y de servicios.

Debe contar con soporte técnico 24x7 escalable hacia la casa matriz incluido en la licencia y en español. Se debe tener un documento del fabricante donde certifique que cuenta con este tipo de soporte así como el número de teléfono de asistencia técnica.

El soporte técnico corresponde a la responsabilidad del fabricante de la solución para dar respuesta y solución a la aparición de un nuevo software malintencionado (virus, spyware, spam, phishing, pharming, etc.) en un plazo inferior a las horas indicadas.

El proveedor demostrará su idoneidad para la ejecución del presente proyecto mediante la presentación de la certificación respectiva expedida por el fabricante y firmada por el respectivo representante legal.

Para la instalación, configuración y puesta en funcionamiento de la solución el fabricante y/o proveedor designará como mínimo un (01) ingeniero experto debidamente certificado por el fabricante de la solución en las tareas mencionadas.

- **Personal y mantenimiento interno.**

La entidad dispone del personal técnico a través de la Sección de Soporte Técnico del Área de Tecnologías de la Información de la Gerencia de Servicios.

- **Capacitación.**

  Se deberá ofrecer un programa de adiestramiento técnico-teórico-práctico para el personal técnico de la entidad, con el propósito de capacitarlos en la Administración, Configuración, Monitoreo y Mantenimiento adecuado de toda la solución de seguridad materia del presente requerimiento.

  La capacitación deberá ser realizada por el fabricante, o por medio de sus canales autorizados. La duración deberá ser de por lo menos 15 horas efectivas.

  La capacitación deberá contener los siguientes temas:

  - Solución de Seguridad Antivirus para Estaciones y Servidores
  - Consola de Administración

- **Costo Operativo de TI.**

  La solución permitirá una reducción de los costos operativos en las infecciones de virus electrónicos que presenta la institución, considerando la dispersión que presenta las dependencias y mejor control de la administración de la red.

- **Impacto en el cambio de plataforma.**

  El impacto del cambio de plataforma es mínimo, puesto que la institución cuenta con una solución provisional de antivirus corporativo con las características técnicas mínimas descritas para las estaciones de trabajo y los Servidores. Por lo que es importante mantener dicha infraestructura de seguridad.

- **Tiempo de Recuperación.**

  Se debe buscar una rápida respuesta, Soporte Técnico las 24 horas del día x 7 días de la semana x 365 días del año, con respuesta en el sitio dentro de las 3 horas de haber recibido la llamada del usuario.

- **Tiempo de entrega de la solución.**

  Este debe ser como mínimo 15 días calendario desde la emisión de la Orden de Compra.

- **Garantías comerciales aplicables.**

  Se debe dar dentro del periodo del contrato con el mantenimiento y soporte técnico respectivo.

ITEM	ATRIBUTOS	Antivirus Nacionales	Antivirus Extranjeros	Puntaje Máximo
01	Licenciamiento	9	9	10
02	Hardware necesario para su funcionamiento	9	9	10
03	Soporte y Mantenimiento Externo	6	8	10
04	Personal y Mantenimiento Interno	9	9	10
05	Capacitación	8	8	10
06	Costo Operativo de TI	9	9	10
07	Impacto en el cambio de Plataforma	9	10	10
08	Tiempo de Recuperación	9	9	10
09	Tiempo de Entrega de la Solución	9	10	10
10	Garantías Comerciales aplicables	9	9	10
	Total	**86**	**90**	**100**

9. CONCLUSIONES

- ✓ Se determinó los atributos o características técnicas mínimas que deben ser considerados para una evaluación de una solución de seguridad de antivirus corporativa, asimismo se estableció la valoración cuantitativa de cada característica.

- ✓ Por lo anteriormente expuesto se considera que el producto a adquirir debe contar con los atributos técnicos descritos en los puntos anteriores, ya que con ello se adaptará a las características de nuestra infraestructura de red corporativa.

- ✓ La entidad requiere comprar 200 licencias de una Solución de Software de Antivirus Corporativo para proteger y controlar las estaciones de trabajo, servidores y equipos portátiles en los distintos puntos de la red con productos de un solo fabricante que contengan los últimos avances tecnológicos.

- ✓ Se requiere las últimas versiones liberadas por el fabricante. No se aceptarán versiones beta, en etapas de desarrollo tempranas o versiones anteriores.

- ✓ La solución ofertada deberá de tener una licencia de suscripción por 01 año con mantenimiento de software, incluye bases de datos de virus, UPDATES y UPGRADES del antivirus ofertado.

10. FIRMAS

Ing. Ivan Rojas Morales
Asistente en Soporte y Software

V°B° Ing. Martin Alcántara Martínez
Especialista en Soporte y Software

V°B° Ing. Carlos Ruiz Cancino
Jefe del Área de Tecnologías de la Información