

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE
N° 01-2013-JRVC-EFPT-GTIC/MSI
ADQUISICIÓN DE LICENCIAS DE SOFTWARE DE ANTIVIRUS

1. NOMBRE DEL AREA
Gerencia de Tecnologías de Información y Comunicación

2. RESPONSABLE DE LA EVALUACION
Sr. Juan Vásquez Carranza

3. CARGO
Especialista en Tecnología de la Información y Comunicaciones

4. FECHA
19 de septiembre de 2013

5. JUSTIFICACION
 - a. Definición de Malware
Se define el MALWARE como la abreviación de los términos en inglés "Malicious Software" (software malintencionado). Se trata de un nombre colectivo que incluye virus, gusanos, caballos de Troya, etc., que realizan expresamente tareas malintencionadas en un sistema informático. Técnicamente un MALWARE es un código malintencionado.

 - b. Clasificación del Malware
Se pueden clasificar en dos tipos, que son:
 - Los que afectan la información, entre ellos tenemos:
 - o Virus
 - o Troyanos
 - o Spyware
 - o Phishing
 - o Back door
 - o Bomba lógica

 - Afectan el rendimiento del equipo de cómputo, como por ejemplo:
 - o Worm
 - o Adware
 - o Rootkit
 - o Denegación de servicios



c. Antimalware

Es un software o programa informático que permite eliminar el software malintencionado.

Se recomienda instalar un programa antivirus en todos los equipos cómputo y servidores, y se debe mantenerse actualizado. Dado que los virus nuevos pueden propagarse sumamente rápido, es importante disponer de una infraestructura de actualización que pueda actualizar todos los equipos con frecuencia y a corto plazo.

Dado que los malware pueden aprovechar la conexión a internet y bajar nuevos códigos maliciosos es necesario complementar la protección con un Firewall que permita bloquear este tipo de acciones y otros ataques informáticos.

Actualmente la Municipalidad de San Isidro (MSI) cuenta con equipos móviles y según los datos estadísticos en el 2013 para sistemas Móviles, en el segundo trimestre se dio un constante aumento desde el primer trimestre, con un total de 29.695 modificaciones (primer trimestre de 2013: 22.749). En abril se detectaron 7.141 modificaciones, lo que representa el punto más bajo en el segundo trimestre. Sin embargo, en mayo y junio detectó más de 11.000 modificaciones (11.399 y 11155, respectivamente). En general, el año 2013 fue testigo de un notable salto en la cantidad de nuevas modificaciones móviles. Estos datos fueron tomados de la url: <http://www.viruslist.com/sp/analysis?pubid=207271222> el día 17 de setiembre del 2012. En el segundo trimestre de este año, detectamos lo que es probablemente el troyano más sofisticado de todos los tiempos dirigido contra Android. Puede enviar mensajes SMS a números de pago, descargar e instalar otros programas maliciosos en el dispositivo infectado y/o enviarlos por Bluetooth, así como ejecutar comandos remotos desde la consola.

Para poder proteger los equipos de la MSI, es necesaria la instalación de un software especializado, que los proteja de los malware, garantizando su operatividad y la comunicación entre los sistemas informáticos.

d. Alternativas de Antimalware:

- i. Alternativa 1 - Software con licencia. Existen una gran variedad de productos. Actualmente la MSI usa antimalware Sophos End Point Security and Control.
- ii. Alternativa 2 - Software Gratuito. Existen en el mercado informático alternativas de este software, como por ejemplo:
 - Microsoft Security Essentials, solo para equipos Windows.



6. ANALISIS COMPARATIVO TECNICO

Con la finalidad de realizar una evaluación técnica se establecerá una selección de métricas según se muestra en la tabla 1: Selección de Métricas

Tabla 1: Selección de Métricas

Ítem	Atributos	Nivel
1	Atributos Internos y Externos	
1.1	Funcionales	20
1.2	Compatibles	20
1.3	Operatividad	20
2	Atributos de Uso	
2.1	Uso y productividad	20
2.2	Eficacia	20

Fuente: Elaboración Propia

Entre los atributos funcionales se evaluará:

- A. Consola de actualización centralizada
- B. Despliegue y actualización remota

Entre los atributos Compatibles se evaluará:

- A. Múltiple plataforma de sistema operativo; es decir que se pueda instalar en Windows, Linux, Android y Mac
- B. Solo una Plataforma

Entre los atributos de Operatividad se evaluará:

- A. Poseer Firewall Personal
- B. Control de Dispositivos
- C. Control de ejecución de aplicaciones

Entre los atributos de Uso y Productividad se evaluará:

- A. Evaluación destacada de líder por empresas terceras (Magic Quadrant Gartner), tanto en protección de equipos de escritorio
- B. Evaluación destacada de líder para móviles MDP (Mobile Data Protection).

Entre los atributos de Eficacia se evaluará:

- A. Poseer herramientas para la remoción de Malware
- B. Que contenga un sistema de protección de fuga de datos (DLP) integrado a la solución antivirus



Tabla 2: Análisis técnico de ambas alternativas

Ítem	Atributos	Nivel	Alternativa 1	Alternativa 2
1	Atributos Internos y Externos			
1.1	Funcionales	20	20	00
1.2	Compatibles	20	20	10
1.3	Operatividad	20	20	10
2	Atributos de Uso			
2.1	Uso y productividad	20	20	05
2.2	Eficacia	20	20	00
		Total	100	25

Fuente: Elaboración propia

7 ANALISIS COSTO-BENEFICIO

Tabla 3: Análisis Costo Beneficio

Alternativa	Precio S/.	Evaluación
1	Mayor a 0.00	000
2	S/. 0.00	100

Fuente: Elaboración Propia

8. CONCLUSIONES

En la consolidación de las tablas se tiene:

Tabla 3: Resumen de evaluación global

Evaluación	Peso	Alternativa 1	Alternativa 2
Análisis Comparativo Técnico	70	70	17.50
Análisis Costo Beneficio	30	00	30.00
	Total	70	47.50

Fuente: Elaboración propia

Del análisis de la información presentado se recomienda la Alternativa 1: Compra de un Software especializado en la protección de Malware.



MUNICIPALIDAD DE SAN ISIDRO

Ángel Alvarado A.

Ángel Alvarado A.
Jefe de Equipo Funcional de Plataforma Tecnológica
Gerencia de Tecnologías de Información y Comunicación