

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE



1. **NOMBRE DEL ÁREA:**
Oficina de Sistemas de Información.
2. **RESPONSABLE(S) DE LA EVALUACIÓN**
Juan Gustavo Torres Sosa.
3. **CARGO(S)**
Responsable de la evaluación del software para el monitoreo de la red del data center
4. **FECHA**
Lima, 03 de Abril del 2017

5. **JUSTIFICACIÓN:**

La adquisición del software para el monitoreo de la red del data center, permitirá monitorear el uso de memoria, procesamiento y discos de los componentes de infraestructura críticos del datacenter del INGEMMET, incluyendo dispositivos de comunicaciones (routers, switches, servidores y todo otro dispositivo administrable), desde una perspectiva de monitoreo predictivo/correctivo de la conectividad de la red y el funcionamiento propio del sistema, permitiendo asegurar la integridad de los servicios de red y comunicaciones.

Se ha procedido a evaluar según lo establecido en la Ley N° 28612, ley que norma el uso, adquisición y adecuación del software en la administración pública, las características más importantes establecidas para el Software de análisis de los datos de calidad del agua

6. **ALTERNATIVAS**

Se ha evaluado los siguientes Software:

- NAGIOS
- OPMANAGER

7. **ANÁLISIS COMPARATIVO TÉCNICO**

Se realizó aplicando la parte 3 de la Guía de Evaluación de Software.

7.1 **Propósito de la Evaluación:**

Determinar las características de calidad mínimas para el producto final, software para el monitoreo de la red del data center.

7.2 **Identificar el tipo de producto.**

Software para el monitoreo de la red del data center requerido por el INGEMMET.

7.3 **Especificación del Modelo de Calidad.**

Se ha aplicado el Modelo de calidad de Software descrito en la Parte 1 de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM.



7.4 Selección de Métricas.

Las métricas han sido seleccionadas en base al análisis de información de requerimiento de Calidad para el software solicitado, los requerimientos de calidad en los niveles técnicos y operativos, y requerimientos de calidad que demanda nuestra arquitectura de Red.

7.4.1 Selección de requisitos de Calidad.

Hemos determinado los siguientes requisitos de calidad que debe de cumplir el software para el monitoreo de la red del data center requerido por el INGEMMET.

Cuadro 7.1

Requisitos de Calidad para el software para el monitoreo de la red del data center para el INGEMMET

CALIDAD	
ITEM	REQUERIMIENTO DE CALIDAD INTERNA
1	Debe permitir el monitoreo de los equipos de red, detectar posibles fallas en la disponibilidad del servicio y sus causas, saturación de memoria, saturación de procesador, saturación de almacenamiento, saturación de red, caída de un servicio o proceso, monitorear los cambios de configuración, los accesos, asignación de políticas de equipos de comunicación, actualización del software, monitoreo de los puertos de conexión y otros.
2	Debe contar con el establecimiento de políticas según el tipo de dispositivo (servidor de base de datos, correo, aplicaciones, impresora de red, equipo de comunicación, UPS y otros).
3	Debe permitir la definición de umbrales a nivel de interfaces de switches de tal manera se pueda identificar cuellos de botella o tráfico sospechoso.
4	Compatibilidad con Servidores: Completa funcionalidad y soporte para sistemas operativos Windows Server (2000, 2003, 2008, 2012 y 2016), Redhat 5, 6 y/o superior, Centos 5 y/o superior.
5	Permite monitorear la disponibilidad y el tiempo productivo de los dispositivos de red.
6	Monitorear el estado de los dispositivos de red tales como router, switches, firewalls, puntos de acceso Wireless.
7	Debe contar con la capacidad de realizar correlación de alarmas-eventos, es decir ante una caída masiva de dispositivos, identifique la falla origen, y no altere sucesivamente por alertas relacionadas a la misma falla reportada.
8	Debe contar con su propia base de datos o base de datos de terceros,
9	Debe Monitorear la disponibilidad y el tiempo de respuesta de los siguientes servicios:DNS, Echo, HTTPS, IMAP, LDAP, SMTP, Telnet, FTP, Web PoP, WebLogic, HTTPS, URL
10	Listar por ID del proceso, nombre, ruta y argumento de proceso.
11	Listar los 10 procesos que más consumen CPU y memoria.
12	Gestión avanzada de fallas, el sistema debe de informar via correo electrónico, alarma web o ejecutar un script o programa.
13	permitir configuración para la finalización de procesos perjudiciales de forma remota
14	Monitorear de las páginas web que requieran un login autenticado
15	Permitir monitorear servidores de múltiples plataformas y sistemas operativos tales como: Windows, Linux, Solaris, Unix, VMware, AIX, HP-UX etc. utilizando SNMP, WMI, CLI y Telnet/SSH independientemente del tipo o la marca de los dispositivos.
16	Monitoreo de servidores virtuales VMware ESX/ ESXi, Hyper-V.
17	Monitorear alertas y eventos de sistemas y aplicaciones – Monitor de servidores IIS, Exchange, etc.
18	Monitoreo integrado de logs de eventos – No necesitará contar con una consola adicional



19	Permitir alertas basadas en umbrales.
20	Permite ejecución automática de scripts.
21	Permitir la configuración de reglas de escalamiento de alarmas automáticas.
REQUERIMIENTOS DE CALIDAD EXTERNA	
22	Para cualquier otro dispositivo, la solución debe permitir la recepción, interpretación y gestión de eventos basados en protocolos SNMP.
23	Adicionalmente la herramienta debe soportar (con licenciamiento adicional), sin integraciones de productos adicionales, las funcionalidades y monitoreo sobre: NetFlow, Sflow, Jflow, QoS Voip (Quality of Service), IPV4 e IPV6, Monitoreo de base de datos, Aplicaciones y procesos, POP, SMTP, IMAP, LDAP.
24	Debe ser capaz de monitorear ambientes virtualizados y soportar las siguientes tecnologías: Hyper-V, VMware ESX / ESXi vía WBem, entre otras.
25	La consola para gestión y administración de la solución debe soportar protocolos de conexión segura (SSL).
26	Monitorear como mínimo los siguientes parámetros de rendimiento de los routers en una sola pantalla: Disponibilidad, Utilización de CPU, Utilización de memoria, Pérdida de Paquetes, Tiempo de Respuesta, Temperatura, Alarmas recientes, Interfaces (Tráfico Ingreso, Tráfico Salida, Errores), Estadísticas de búfer (Hits, Misses, Fails)
27	La herramienta deberá contar con función de reportes integrados, sin la necesidad de agregar producto de terceros, ni módulos adicionales. La herramienta deberá contar con reportes pre definidos, los cuales deberán poder ser exportados a Excel y pdf. La herramienta de reportes, deberá contar con la funcionalidad de programación automatizada de reportes, para la ejecución envío y publicación de manera automática y desatendida.
28	Debe monitorear los servidores: utilización de CPU, espacio del disco, temperatura, estado del ventilador, tiempo de respuesta, pérdida de paquetes, disponibilidad.
29	Debe monitorear los servicios de Windows sin agentes via WMI: DHCP Server, Disk Manager, DNS Server, Event Log, IAS, IIS, Messenger, MySQL, Net Logon, Print Spooler, RPC, Telephony:
30	Descubrir y listar los procesos ejecutados en los dispositivos descubiertos, procesos corriendo sobre servidores Windows, Linux, Solaris, Unix, HP UX, IBM AIX, ESX VMware.
31	Permitir la configuración de umbrales individuales para los parámetros monitoreados.
32	Debe emitir Reportes de tendencias de procesos del día, del día anterior, la última semana, el último mes o un periodo de tiempo personalizado.
33	Debe contar con plantilla de procesos para asociar procesos a múltiples dispositivos.
34	Monitoreo de Syslog y procesamiento de SNMP Trap
35	Método basado en reglas para leer syslogs entrantes y asignar estos syslogs para notificar al personal de red correspondiente o para realizar otras tareas, por ejemplo, el apagado de un servidor o un puerto.
36	Admitir una gran cantidad de dispositivos en múltiples plataformas, por ejemplo, cualquier dispositivo de exportación de syslogs o cualquier aplicación (servidores Linux, UNIX, AIX y Solaris; routers, switches, etc.).
37	Los operadores podrán especificar las reglas de umbrales para un servicio, una aplicación o un dispositivo y programar una regla para recibir alertas en caso de violación de una regla de umbrales.
38	Debe de tener informes predefinidos y permitir la personalización.
39	Generar informes de rendimiento de la red, envío automático y programado de informes periódicos vía email
REQUERIMIENTO DE CALIDAD DE USO	
40	Deber ser del tipo "Agent Less", es decir no habrá la necesidad de instalar agentes remotos, en los equipos o dispositivos a monitorear.
41	Debe contar con la capacidad de armar mapas topológicos de la infraestructura descubierta y generar las relaciones entre ellos.



42	Permitir la gestión de monitoreo SNMP personalizados para monitorear otras estadísticas de rendimiento importantes de los equipos.
43	Permite el mapeo automático de la red agrupando los dispositivos descubiertos y ofrecer vistas de red basados en el tipo de infraestructura (switches, servidores, routers, etc.) el tipo de proveedor (HP, Extreme, Alcatel, Cisco, IBM, Fortinet, etc.) y los grupos de red (capa 3).
44	Permitir la configuración de flujos de trabajo automáticos para la ejecución de trabajos como reiniciación de servicios caídos, reseteo de equipos y emitir alertas a los administradores del sistema.
45	Permitir monitoreo del estado del sistema (CPU, memoria, disco, estado del hardware, temperatura)
46	Monitoreo de archivos y folders a través de parámetros de antigüedad y cambios realizados
47	Monitorear alertas, eventos de Windows y/o eventos de seguridad.
48	Permitir la integración automatizada con una herramienta de mesa de ayuda.
49	Administración avanzada de alertas (Configure la dependencia de los dispositivos, programe el tiempo de inactividad, suprima alarmas/escalamiento)
50	Debe permitir acceso remoto vía WAN o desde un dispositivo móvil, a través de un App Móvil disponible para iPhone, iPad y Android.

7.4.2. Selección de atributos de Calidad.

Los atributos de calidad que se utilizarán para la evaluación del software para el monitoreo de la red del data center requerido por el INGEMMET, de acuerdo a lo especificado en la parte 2 de la Guía de Evaluación de Software se muestran en el siguiente cuadro:

Cuadro 7.2

Atributos de calidad tomados en cuenta en la Evaluación	
ATRIBUTOS INTERNOS	Características del Software que determinan su habilidad para satisfacer las necesidades propias e implícitas.
ATRIBUTOS EXTERNOS	Características del Software que determinan su habilidad para satisfacer las necesidades explícitas e implícitas
ATRIBUTOS EN USO	Características del Software que determinan los requerimientos de los usuarios finales de manera que satisfagan sus necesidades

7.4.3 Asignación de puntajes a los atributos de Calidad.

Los puntajes establecidos a los atributos de calidad seleccionados de acuerdo a nuestras necesidades se muestran en el siguiente cuadro:

Cuadro 7.3

Métricas adoptadas de acuerdo a la Necesidad	
Tipo de Atributo	Puntaje
ATRIBUTOS INTERNOS	45
ATRIBUTOS EXTERNOS	36
ATRIBUTOS EN USO	19
TOTAL	100

Nota: La escala de evaluación que se ha tomado es de 1 a 100

Evaluación de los criterios de calidad para las alternativas de software para el monitoreo de la red del data center requerido por el INGEMMET tomados como referencia.



Cuadro 7.4
Evaluación de criterios de Calidad

CALIDAD		CALIFICACIÓN		
ITEM	REQUERIMIENTO DE CALIDAD INTERNA	Puntaje Max	INAGIOS	DEMANAGER
1	Debe permitir el monitoreo de los equipos de red, detectar posibles fallas en la disponibilidad del servicio y sus causas, saturación de memoria, saturación de procesador, saturación de almacenamiento, saturación de red, caída de un servicio o proceso, monitorear los cambios de configuración, los accesos, asignación de políticas de equipos de comunicación, actualización del software, monitoreo de los puertos de conexión y otros.	3	3	3
2	Debe contar con el establecimiento de políticas según el tipo de dispositivo (servidor de base de datos, correo, aplicaciones, impresora de red, equipo de comunicación, UPS y otros).	2	2	2
3	Debe permitir la definición de umbrales a nivel de interfaces de switches de tal manera se pueda identificar cuellos de botella o tráfico sospechoso.	2	1	2
4	Compatibilidad con Servidores: Completa funcionalidad y soporte para sistemas operativos Windows Server (2000, 2003, 2008, 2012 y 2016), Redhat 5, 6 y/o superior, Centos 5 y/o superior.	3	3	3
5	Permite monitorear la disponibilidad y el tiempo productivo de los dispositivos de red.	2	2	2
6	Monitorear el estado de los dispositivos de red tales como router, switches, firewalls, puntos de acceso Wireless.	2	2	2
7	Debe contar con la capacidad de realizar correlación de alarmas-eventos, es decir ante una caída masiva de dispositivos, identifique la falla origen, y no altere sucesivamente por alertas relacionadas a la misma falla reportada.	2	2	2
8	Debe contar con su propia base de datos o base de datos de terceros,	1	1	1
9	Debe Monitorear la disponibilidad y el tiempo de respuesta de los siguientes servicios: DNS, Echo, HTTPS, IMAP, LDAP, SMTP, Telnet, FTP, Web PoP, WebLogic, HTTPS, URL	2	1	2
10	Listar por ID del proceso, nombre, ruta y argumento de proceso.	1	1	1
11	Listar los 10 procesos que más consumen CPU y memoria.	2	1	2
12	Gestión avanzada de fallas, el sistema debe de informar vía correo electrónico, alarma web o ejecutar un script o programa.	2	2	2
13	permitir configuración para la finalización de procesos perjudiciales de forma remota	2	1	2
14	Monitorear de las páginas web que requieran un login autenticado	2	1	2
15	Permitir monitorear servidores de múltiples plataformas y sistemas operativos tales como: Windows, Linux, Solaris, Unix, VMware, AIX, HP-UX etc. utilizando SNMP, WMI, CLI y Telnet/SSH independientemente del tipo o la marca de los dispositivos.	3	2	3
16	Monitoreo de servidores virtuales VMware ESX/ ESXi, Hyper-V.	3	2	3
17	Monitorear alertas y eventos de sistemas y aplicaciones – Monitor de servidores IIS, Exchange, etc.	3	2	3
18	Monitoreo integrado de logs de eventos – No necesitará contar con una consola adicional	2	2	2
19	Permitir alertas basadas en umbrales.	2	2	2
20	Permite ejecución automática de scripts.	2	2	2
21	Permitir la configuración de reglas de escalamiento de alarmas automáticas.	2	1	2
REQUERIMIENTOS DE CALIDAD EXTERNA				



22	Para cualquier otro dispositivo, la solución debe permitir la recepción, interpretación y gestión de eventos basados en protocolos SNMP.	2	2	2
23	Adicionalmente la herramienta debe soportar (con licenciamiento adicional), sin integraciones de productos adicionales, las funcionalidades y monitoreo sobre: NetFlow, Sflow, Jflow, QoS Voip (Quality of Service), IPV4 e IPV6, Monitoreo de base de datos, Aplicaciones y procesos, POP, SMTP, IMAP, LDAP.	4	2	4
24	Debe ser capaz de monitorear ambientes virtualizados y soportar las siguientes tecnologías: Hyper-V, VMware ESX / ESXI vía WBem, entre otras.	2	2	2
25	La consola para gestión y administración de la solución debe soportar protocolos de conexión segura (SSL).	2	2	2
26	Monitorear como mínimo los siguientes parámetros de rendimiento de los routers en una sola pantalla: Disponibilidad, Utilización de CPU, Utilización de memoria, Pérdida de Paquetes, Tiempo de Respuesta, Temperatura, Alarmas recientes, Interfaces (Tráfico Ingreso, Tráfico Salida, Errores), Estadísticas de búfer (Hits, Misses, Fails)	2	2	2
27	La herramienta deberá contar con función de reportes integrados, sin la necesidad de agregar producto de terceros, ni módulos adicionales. La herramienta deberá contar con reportes pre definidos, los cuales deberán poder ser exportados a Excel y pdf. La herramienta de reportes, deberá contar con la funcionalidad de programación automatizada de reportes, para la ejecución envío y publicación de manera automática y desatendida.	2	1	2
28	Debe monitorear los servidores: utilización de CPU, espacio del disco, temperatura, estado del ventilador, tiempo de respuesta, pérdida de paquetes, disponibilidad.	2	2	2
29	Debe monitorear los servicios de Windows sin agentes vía WMI: DHCP Server, Disk Manager, DNS Server, Event Log, IAS, IIS, Messenger, MySQL, Net Logon, Print Spooler, RPC, Telephony:	2	1	2
30	Descubrir y listar los procesos ejecutados en los dispositivos descubiertos, procesos corriendo sobre servidores Windows, Linux, Solaris, Unix, HP UX, IBM AIX, ESX VMware.	2	2	2
31	Permitir la configuración de umbrales individuales para los parámetros monitoreados.	2	2	2
32	Debe emitir Reportes de tendencias de procesos del día, del día anterior, la última semana, el último mes o un período de tiempo personalizado.	2	2	2
33	Debe contar con plantilla de procesos para asociar procesos a múltiples dispositivos.	2	2	2
34	Monitoreo de Syslog y procesamiento de SNMP Trap	1	1	1
35	Método basado en reglas para leer syslogs entrantes y asignar estos syslogs para notificar al personal de red correspondiente o para realizar otras tareas, por ejemplo, el apagado de un servidor o un puerto.	2	2	2
36	Admitir una gran cantidad de dispositivos en múltiples plataformas, por ejemplo, cualquier dispositivo de exportación de syslogs o cualquier aplicación (servidores Linux, UNIX, AIX y Solaris; routers, switches, etc.).	2	2	2
37	Poder especificar las reglas de umbrales para un servicio, una aplicación o un dispositivo y programar una regla para recibir alertas en caso de violación de una regla de umbrales.	2	2	2
38	Debe de tener informes predefinidos y permitir la personalización.	1	1	1
39	Generar informes de rendimiento de la red, envío automático y programado de informes periódicos vía email	2	2	2
REQUERIMIENTO DE CALIDAD DE USO				
40	Deber ser del tipo "Agent Less", es decir no habrá la necesidad de instalar agentes remotos, en los equipos o dispositivos a monitorear.	1	1	1



41	Debe contar con la capacidad de armar mapas topológicos de la infraestructura descubierta y generar las relaciones entre ellos.	2	1	2
42	Permitir la gestión de monitoreo SNMP personalizados para monitorear otras estadísticas de rendimiento importantes de los equipos.	2	2	2
43	Permite el mapeo automático de la red agrupando los dispositivos descubiertos y ofrecer vistas de red basados en el tipo de infraestructura (switches, servidores, routers, etc.) el tipo de proveedor (HP, Extreme, Alcatel, Cisco, IBM, Fortinet, etc.) y los grupos de red (capa 3).	2	2	2
44	Permitir la configuración de flujos de trabajo automáticos para la ejecución de trabajos como reiniciación de servicios caídos, reseteo de equipos y emitir alertas a los administradores del sistema.	2	2	2
45	Permitir monitoreo del estado del sistema (CPU, memoria, disco, estado del hardware, temperatura)	1	1	1
46	Monitoreo de archivos y folders a través de parámetros de antigüedad y cambios realizados	1	1	1
47	Monitorear alertas, eventos de Windows y/o eventos de seguridad.	2	2	2
48	Permitir la integración automatizada con una herramienta de mesa de ayuda.	2	0	2
49	Administración avanzada de alertas (Configure la dependencia de los dispositivos, programe el tiempo de inactividad, suprima alarmas/escalamiento)	2	1	2
50	Debe permitir acceso remoto vía WAN o desde un dispositivo móvil, a través de un App Móvil disponible para iPhone, iPad y Android.	2	0	2
Totales		100	81	100

Nota: La escala de evaluación que se ha tomado es de 1 a 10

8. ANÁLISIS COMPARATIVO COSTO – BENEFICIO

Para la elaboración del análisis de costo beneficio se han tomado en cuenta los criterios solicitados en el punto 8 del reglamento de la Ley N° 28612, los cuales son:

Criterios mínimos:

- Licenciamiento
- Hardware necesario para su funcionamiento
- Soporte y mantenimiento externo
- Personal y mantenimiento interno
- Capacitación

Criterios adicionales:

- Impacto en el cambio de plataforma.
- Garantías Comerciales Aplicables.

Estos criterios se expresan en el siguiente cuadro:

Cuadro 8.1

ITEM	Criterios a Evaluar	NAGIOS	OPMANAGER
1	Licenciamiento	No Requiere	Requiere
2	Cantidad de Licencias referenciales	1	1
3	Costo referencial en Nuevos Soles, por la cantidad de Licencias requeridas	S/0.00	S/. 2,308.00
4	Hardware Necesario para su Funcionamiento	Intel / AMD, 1.5 Ghz, 2 GB de. RAM, 2 GB de espacio libre en Disco Duro, Adaptador de video SVGA	Intel / AMD, 1.5 Ghz, 2 GB de. RAM, 2 GB de espacio libre en Disco Duro, Adaptador de video SVGA



5	Soporte y Mantenimiento Externo	No Requiere	No Requiere
6	Personal y mantenimiento Interno	No Requiere	No Requiere
7	Capacitación para el Uso del Software de monitoreo de red	Requerido para el personal encargado	Requerido para el personal encargado
8	Costo referencial, en Nuevos Soles, por Capacitación para la cantidad de personal que se especifica.	S/. 0.00	S/. 0.00
9	Garantía Comercial	No hay Garantía Comercial	El proveedor proporciona Garantía Comercial
10	Impacto en el cambio de la Plataforma	Habría un impacto mediano, No existe experiencia en el uso del software	No habría Impacto porque hay experiencia en el uso del software.

8.1 Asignación de puntajes para los criterios a evaluar

Para poder medir los criterios indicados en el Cuadro 8.1 se ha elaborado una escala de puntajes y pesos para cada criterio, las cuales se indican en el siguiente cuadro:

Cuadro 8.2

Escala de puntajes y pesos

ITEM	PARAMETRO (Referido al Elemento a evaluar)	PUNTAJE	PESO
1	REQUIERE	0	1
	NO REQUIERE	10	
2	MAYOR CANTIDAD DE LICENCIAS	0	1
	IGUAL CANTIDAD DE LICENCIAS	5	
	MENOR CANTIDAD DE LICENCIAS	10	
3	MENOR COSTO	10	1
	MAYOR COSTO	0	
4	MENOS HARDWARE	10	1
	IGUAL HARDWARE	5	
	MAYOR HARDWARE	0	
5	REQUIERE	0	1
	NO REQUIERE	10	
6	REQUIERE	0	1
	NO REQUIERE	10	
7	PARA TODO EL PERSONAL	0	1
	SOLO PARA PERSONAL TECNICO	10	
8	MENOR COSTO	10	3
	MAYOR COSTO	0	
9	SE PROPORCIONA GARANTIA	10	3
	NO SE PROPORCIONA GARANTIA	0	
10	ALTO IMPACTO	0	10
	MEDIANO IMPACTO	5	
	NO HAY IMPACTO	10	

Nota 1: Los ítem del cuadro 8.2 son los mismos a los del cuadro 8.1

Nota 2: La escala de evaluación que se ha tomado es de:

- de 1 a 10 para los puntajes
- de 1 a 10 para los pesos



8.2 Resultados de la Evaluación

El cuadro que a continuación se muestra es el resultado de la evaluación de costo beneficio del Software para el monitoreo de la red del data center.

Cuadro 8.3

RESULTADOS DE EVALUACIÓN DE COSTO BENEFICIO

ITEM	Criterios a Evaluar	NAGIOS	OPMANAGER
1	Licenciamiento	10	0
2	Cantidad de Licencias	5	5
3	Costo referencial en Nuevos Soles, por la cantidad de licencias requeridas	10	0
4	Hardware Necesario para su Funcionamiento	5	5
5	Soporte y Mantenimiento Externo	10	10
6	Personal y mantenimiento Interno	10	10
7	Capacitación para el Uso del Software	10	10
8	Costo referencial, en Nuevos Soles, por Capacitación para la cantidad de personal que se especifica.	30	30
9	Garantía Comercial	0	30
10	Impacto en el cambio de la Plataforma	50	100
Puntaje Total		140	200


Nota1: Los ítem del cuadro 8.3 son los mismos a los del cuadro 8.1 y cuadro 8.2


Nota2: Los valores resultados en el cuadro 8.3 están referidos al cálculo PUNTAJE x PESO del cuadro 8.2

9. CONCLUSIONES

- De acuerdo con la evaluación de los criterios de calidad requeridos para el INGEMMET, los cuales se indican en el Cuadro 7.4; para el **Software para el monitoreo de la red del data center**, el que cumple con un mayor número de criterios de calidad es el software **OPMANAGER**.
- De acuerdo con la evaluación de los criterios tomados en cuenta para el análisis de costo beneficio, los cuales se indican en el Cuadro 8.3; se debe optar por el **Software para el monitoreo de la red del data center** que brinda mayores beneficios para el INGEMMET, este es el software **OPMANAGER** por obtener el mayor puntaje en la evaluación de costo beneficio.

10. FIRMAS

Responsable	Firma
Ing. Juan Torres Sosa Responsable de la evaluación	

Responsable de la Aprobación	Firma
Miriam Araya Carrasco. Directora (e) de la Oficina de Sistemas de Información.	 Ing. MIRIAM ARAYA CARRASCO DIRECTORA (e) Oficina de Sistemas de Información INGEMMET