INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE Nº 006-2021-Sunat/1U4200/AX73

1. **NOMBRE DEL ÁREA**

   DIVISION DE ARQUITECTURA TECNOLOGICA

2. **RESPONSABLE DE LA EVALUACIÓN**

   HECTOR ONOFRIO RAMOS CHAVEZ

3. **CARGO**

   ARQUITECTO DE INFRAESTRUCTURA TI

4. **FECHA**

   19/02/2021

5. **JUSTIFICACIÓN**

   En la actualidad la entidad posee la herramienta System Center Configuration Manager (SCCM) para la gestión de parches para productos Microsoft en entornos on premise y no se cuenta con alguna otra herramienta para sistemas operativos Linux, Unix y AIX tampoco herramientas para gestión de parches para soluciones en nube.

   La entidad requiere la adquisición de una solución para el descubrimiento de infraestructura tecnológica y una solución para patch management que permita al personal de los negocios aduanero y tributario garantizar la disponibilidad tecnológica con capacidad de monitoreo y gestión centralizado bajo los estándares de ISO 27001 e ISO 27032 en cumplimiento al marco de ciberseguridad en la gestión de riesgos las cuales debe abarcar la totalidad de plataformas (Microsoft, Linux, Unix y AIX) en sus diversas modalidades de despliegue (on premise, cloud interno o externo a la institución).

   La implementación de la solución para el descubrimiento de infraestructura tecnológica y la solución para patch management permitirá a la SUNAT aprovechar de forma efectiva los equipos de comunicación y las equipos endpoint, el cual facilitará la toma de decisiones y accesos a la información en tiempo real contribuyendo con el contribuyente para acceder a los servicios de la Sunat, y por lo tanto una atención al contribuyente más eficiente con la finalidad de brindar un servicio de excelencia de clase mundial. Asimismo, dicho modelo permite ejecutar acciones que induzcan y faciliten el cumplimiento de las obligaciones tributarias y aduaneras, incrementando los niveles de recaudación.

6. **ALTERNATIVAS**

   Se evaluarán las siguientes alternativas para la adquisición de las soluciones de descubrimiento de infraestructura tecnológica y Patch Management:

   - BMC Client Management
   - System Center Configuration Manager y Operation Manager

   Para poder realizar la evaluación se están considerando las siguientes métricas:

ESCALA	VALOR
Supera el requerimiento	4
Cumple el requerimiento	2
No Cumple el requerimiento	0

El puntaje mínimo de aprobación de las soluciones de descubrimiento de infraestructura tecnológica debe ser 44 y Patch Management deberá ser 150 (las soluciones de descubrimiento de infraestructura tecnológica y Patch Management deberá cumplir como mínimo el 100% de todas las características mencionadas en el punto de análisis comparativo técnico, en relación al soporte técnico de la solución podrán considerar un partner que cuente con la certificación de la marca que garantice el cumplimiento de lo descrito como requisito de la solución ofertada considerando como valor la escala “Cumple el requerimiento”).

7. ÁNALISIS COMPARATIVO TÉCNICO

Para realizar la comparación de los criterios de evaluación se han considerado las siguientes características técnicas:

Descubrimiento de infraestructura	**Engine Management**	**System Center**
Características generales		
La solución debe contemplar un servidor físico/virtual para su implementación, debe ser rackeable.	2	2
La solución debe descubrir todo equipo informático conectado a la red Sunat con los siguientes criterios; Servidores y estaciones de trabajo con despliegue de agentes y para equipos de networking como Switches, router, firewalls a través de protocolo SNMP (puerto161 y/o 162 versiones v1, v2 y v3), y/o WMI (puerto 135) y/o telnet (puerto 23) y/o SSH (puerto 22).	2	2
Debe permitir identificar vulnerabilidades en el firmware del dispositivo de red e indicar la referencia, obtenida de una base de datos de vulnerabilidad actualizada.	2	2
Debe ser capaz de configurar los periodos de rastreo (descubrimiento) de la red (Se debe determinar horarios donde no afecte rendimiento de los equipos).	2	2
La solución debe contemplar las características de llave en mano, por tanto, el ofertante debe provisionar el licenciamiento necesario para el equipamiento indicado en el ***Anexo I - Parque Informático*** además del Hardware y Software	2	2
El software debe ser No-intrusivo, no debe afectar el rendimiento del mismo.	2	2
El proceso de captura debe ser programado de forma individual o grupal	2	2
La solución a proponer debe obtener y mostrar la relación entre los nodos y las máquinas virtuales por cada servidor.	2	2
El descubrimiento de activos debe permitir la importación desde el Active Directory para obtener rangos de IP´s y/o Vlans.	2	2
La programación de descubrimiento de activos debe permitir agregar nuevos dispositivos automáticamente.	2	2
Debe permitir escanear activos distribuidos en múltiples sitios.	2	2
Debe permitir crear una estructura de credenciales para ser reutilizados en el escaneo y descubrimiento de activos.	2	2
Informes		
El módulo de informes debe permitir crear informes personalizados a partir de consultas en donde se muestren todas las columnas de la base de datos de la solución en referencia (ejemplo con formato tabular y matricial)	2	2
Debe permitir realizar informes de auditorías de activos como cambios de estado en hardware y software.	2	2

Debe soportar la exportación de informes a formatos como csv, xls u otros. El acceso a los informes debe basarse en roles.	2	2
Desde el portal debe mostrar el esquema de base de datos que permita crear querys y/o consultar los datos de manera intuitiva.	2	2
Debe permitir la gestión de inventario del parque informático, censando el hardware y software que lo compone.	2	2
Total	32	32
Características especificas		
Plataforma Microsoft, Linux, AIX	2	2
Software de virtualización VMware ESXi 5.5 y versiones superiores	2	2
Sistemas operativos IBM AIX 5.1, y versiones superiores Linux RedHat 3, y versiones superiores. CentOS 4, 5, 6, 7 y versiones superiores Oracle Linux 4/5 y versiones superiores SLES 11, y versiones superiores Windows Server 2000 y versiones superiores Windows vista, 7, versiones superiores	2	2
Base de Datos Oracle Database Enterprise Edition 11.2.0.4 y versiones superiores Informix Database 11.7 y versiones superiores Kafka 1.1.0 y versiones superiores MongoDB 4.0.8, y versiones superiores. Teradata 15.00 y versiones superiores. Big data – Hive 3.1.0 y versiones superiores. Big data – Hbase 2.0.0 y versiones superiores.	2	2
Equipos End point PC de escritorio. Impresoras Equipos móviles Tablets Teléfonos IP Cámaras IP Proyectores	2	2
Equipos net working Firewall Router Switches Access point	2	2
Subtotal	12	12
Descubrimiento Sub Total	**44**	**44**

Patch management	**Engine Management**	**System Center**
Características generales		
La solución debe contemplar un servidor físico/virtual para su implementación, debe ser rackeable.	2	2
La solución debe gestionar los upgrade a través de roles aprobadores que permitan asegurar su despliegue en ambiente productivos previamente validados por todos los actores.	2	2
La solución debe permitir la reversión de parches fallidos	2	2

La solución debe permitir realizar la reversión a demanda en caso luego de su ejecución algún servicio no funcione correctamente	2	2
La solución debe ser una aplicación web y debe ser posible su acceso por cualquier browser, sin que ello vulnere la seguridad.	2	2
Debe incluir su propia base de datos	2	2
Debe permitir realizar copias de seguridad de la base de datos, configuración, eventos, acciones e historial de la solución patch management de forma programada. Que permiten recuperar la operación, sin perder registro de los parches aplicados.	2	2
Debe permitir gestionar end point en LAN y WAN.	2	2
Debe permitir conectarse a un servidor intermediario que tenga la función de gateway para evitar que el servidor tenga salida directamente.	2	2
• La solución debe garantizar la protección del día cero, para ello deberá: o Proponer un Sistema y/o servicio igual o similar a IDS/IPS. La misma que puede ser embebida o un AddOn a la solución principal. o Debe brindar protección a activos que no tienen soporte (legacy). o Debe realizar protección antes del parche oficial. o Debe tener alertas tempranas (a nivel de red y/o perímetro). o Debe permitir la creación de políticas y/o importarlas del active directory. o Se aceptarán propuestas de protección perimetral y/o despliegue de agentes.	2	2
Debe incluir una aplicación móvil sin costo adicional, que permita realizar seguimiento y visualizar el estado del parchado en el parque informático.	2	2
Debe soportar arquitectura distribuida, servidores distribuidos a fin de realizar los despliegues de forma local u oficina remotas.	2	2
Debe permitir definir el horario y ancho de banda utilizado para la replicación de repositorios de diferentes oficinas remotas.	2	2
La solución debe conectarse automáticamente al equipo con el servidor distribuido según el sitio que se encuentre, el criterio a utilizar es la IP.	2	2
Debe soportar API para la integración de terceras aplicaciones.	2	2
Debe permitir importar certificados SSL para habilitar https.	2	2
Permitir la gestión de activos de forma centralizada (la solución debe descargar las actualizaciones a través de internet y luego desplegar según reglas del negocio).	2	2
Permitir el despliegue de software, instalación de actualizaciones y/o parches.	2	2
Permitir programación de despliegue de software por tipo de equipo.	2	2
Debe permitir consolidar soluciones de seguridad para servidores y estaciones de trabajo a través de agentes y/o SSH u otro previamente autorizado por el área usuaria.	2	2
Permitir la creación de roles para la operación (administración y aprobaciones), y auditoria de la solución.	2	2
Permitir la configuración de paquetes múltiples.	2	2
Permitir el despliegue desatendido de parches.	2	2
Permitir la distribución automatizada de parches pre aprobados.	2	2
Monitorear el parque informático (validar comunicación entre el equipo y la central).	2	2

Emitir reportes y dashboard customizables de acuerdo a la necesidad de la institución.	2	2
Programar y emitir reportes de rangos y periodos personalizados.	2	2
El software debe permitir la creación y despliegue de imágenes para plataformas Windows y Linux en las versiones soportadas por el fabricante,	2	2
Debe permitir desplegar controladores de dispositivos.	2	2
Debe permitir crear un medio de arranque (booteable).	2	2
Gestión de configuración		
La solución debe votable permitir gestionar y desplegar configuraciones de forma masiva y desatendida a sistemas operativos Windows, Linux por usuario, estación de trabajo o servidor.	2	2
Debe permitir visualizar en la consola y notificar de forma periódica el estado de las configuraciones desplegadas.	2	2
Debe permitir mover, copiar, eliminar o renombrar carpetas o archivos de forma masiva y remota.	2	2
Debe permitir aplicar configuraciones en productos de Office.	2	2
Debe permitir aplicar configuraciones en el firewall de Windows.	2	2
Debe permitir crear accesos directos de aplicaciones.	2	2
Debe permitir desplegar configuraciones, por equipo, para cambiar los permisos de carpetas o archivos.	2	2
Debe permitir crear un repositorio de scripts o secuencias de comandos para desplegar.	2	2
Debe permitir la ejecución de scripts personalizados.	2	2
Distribución de software		
Debe permitir instalar o desinstalar software basado en MSI o EXE de forma masiva y desatendida, es decir, debe ser transparente para el usuario final.	2	2
Debe permitir ejecutar actividades o comandos previos y posteriores a la instalación.	2	2
Debe permitir definir directivas de implementación para determinar los días, la hora y rango de tiempo en la cual se ejecutará el despliegue de software	2	2
Debe permitir crear un repositorio de software.	2	2
Debe permitir la creación de paquetes de software basada en plantillas	2	2
Debe permitir publicar un portal de autoservicio para que los usuarios finales puedan acceder a un catálogo a fin de instalar un software de manera automática y que no requiera aprobación.	2	2
Gestión de parches		
Debe permitir desplegar parches a servidores Windows y las aplicaciones de Microsoft de forma masiva y desatendida.	2	2
Debe permitir desplegar parches a servidores Linux de forma masiva y desatendida.	2	2
Debe permitir desplegar parches de aplicaciones de terceros como Java, Adobe, Firefox, office, como mínimo.	2	2
Debe permitir configurar grupos de servidores o estaciones de trabajo por diversos criterios para las pruebas de parches en un ambiente controlado a fin de evaluar su impacto y aprobar o rechazar parches seleccionados según los resultados.	2	2
Debe permitir visualizar en la consola y notificar de forma periódica el estado de los parches desplegados. Debe permitir definir como se realizarán los reinicios si el parche a desplegar lo requiere.	2	2
Debe permitir configurar la Implementación de parches de forma automática: Escaneo, Descarga y Despliegue de Parches.	2	2

Debe permitir identificar los parches faltantes, instalados y aplicables para las plataformas Windows y Linux como mínimo.	2	2
Debe permitir desplegar configuraciones que deshabilite las actualizaciones automáticas en aplicaciones o sistemas operativos.	2	2
La solución debe tener la capacidad de configuración e integración con zonas DMZ, previa coordinación con la DGIT	2	2
Gestion de dispositivos móviles		
Despliegues de perfiles/políticas o La administración de dispositivos debe soportar IOs, Android, Windows y Chrome. o Debe permitir definir políticas para el password utilizado para desbloquear dispositivos. o Debe permitir el despliegue de políticas o perfiles para aplicar restricciones en las aplicaciones de los dispositivos gestionados, como impedir uso de youtube, Gmail, etc. además desinstalar aplicaciones que están en lista negra o instalar aplicaciones aprobadas. o Debe permitir gestionar la SD card. o Debe permitir configurar en el dispositivo perfiles de wifi. o Debe permitir desplegar configuraciones de VPN en el dispositivo. o Debe permitir desplegar configuraciones para el correo electrónico. o El software debe poder habilitar el modo quiosco para limitar el acceso a sólo determinadas aplicaciones. o Debe permitir definir una lista blanca o negra de URLs o páginas web. o La solución debe mostrar el estado de despliegue de los perfiles o políticas. o La solución debe aplicar grupos de políticas o restricciones en el dispositivo según su ubicación. o Debe permitir la creación de grupos personalizadas para aplicación de perfiles de forma masiva. o Debe permitir la actualización del OS del dispositivo.	2	2
Gestion de aplicaciones o La solución debe tener la capacidad de distribuir aplicaciones corporativas y de la tienda de aplicaciones. o Debe permitir publicar aplicaciones en un catálogo de aplicaciones. o La solución debe mostrar el estado de las aplicaciones implementadas. o Debe permitir / evitar copias de seguridad de datos de aplicaciones. o Debe permitir definir una lista negra de aplicaciones. o Debe permitir / denegar que el usuario acepte TLS no confiables. o Debe detectar los dispositivos que están rooteados con jail Break o custom ROMs.	2	2
Informes o Debe emitir reportes que muestre el estado de enrolamiento de dispositivo. o Reportes de inventario de hardware de los dispositivos. o Reportes de inventario de aplicaciones. o Reporte que muestre dispositivos rooteados. o Reportes de seguridad que muestre con aplicaciones en lista negra.	2	2
Herramienta y control remoto		
Debe permitir el encendido y apagado remoto a demanda o de forma programada de una o varias estaciones o servidores	2	2
Debe permitir publicar anuncios por medio del agente a los equipos gestionados (estaciones, servidores y móviles).	2	2

Debe permitir administrar el equipo: iniciar o parar procesos o servicios, ejecutar comandos, tener accesos al visor de eventos, de los equipos gestionados (estaciones, servidores y móviles).	2	2
Debe permitir la programación de herramientas de mantenimiento como limpieza o desfragmentación de disco de los equipos gestionados (estaciones, servidores y móviles).	2	2
Debe permitir el control remoto de un servidor o una estación de trabajo.	2	2
Debe solicitar el consentimiento de los usuarios antes de conectarse a una estación, a fin de proteger su privacidad.	2	2
Debe permitir la transferencia de archivos hacia los equipos gestionados (estaciones, servidores y móviles).	2	2
Debe permitir iniciar un chat y guardar el historial de la conversación hacia los equipos gestionados (estaciones, servidores y móviles).	2	2
Debe permitir grabar las sesiones remotas hacia los equipos gestionados (estaciones, servidores y móviles).	2	2
Informes		
Debe permitir crear informes personalizados y/o permitir crear informes por query	2	2
Debe permitir programar reportes.	2	2
Debe permitir exportar reportes de AD: informes de usuarios, computadoras, grupos, OUs, etc.	2	2
Debe permitir exportar reportes en .xls, .csv y .pdf	2	2
Sub Total	136	136
CARACTERÍSTICAS TÉCNICAS ESPECÍFICAS		
Plataforma Microsoft, Linux	2	2
Software de virtualización La actualización de software virtuales debe aplicarse sobre las versiones vigentes que cuenten con el soporte del fabricante.	2	2
Sistemas operativos Linux RedHat 3, y versiones superiores. CentOS 4, 5, 6, 7 y versiones superiores Debian GNU y versiones superiores Oracle Linux 4/5 y versiones superiores SLES 11, y versiones superiores Windows Server 2000 y versiones superiores Windows vista, 7, versiones superiores	2	2
Equipo end point PC de escritorio mínimo	2	2
Debe identificar mínimamente a un parche y/o actualización con las siguientes características: • Nombre • Serialnumber • Manufacture • MAC Adress • IP Adress • AD Site • Operating System • Service Pack	2	2
Debe soportar mínimo los tipos de transmisión multicast y unicast.	2	2
Sub total	12	12
Patch Sub Total	**148**	**148**

Soporte de solución	Engine Management	System Center
Soporte técnico local	2	2
Soporte 24/7	2	2
Monitoreo de performance de red	4	2
Monitoreo de la salud del hardware	2	2
Monitoreo de aplicaciones	0	4
Monitoreo de base de datos	2	2
Mapeo y establecimiento de umbrales de dependencia de aplicaciones	2	4
Integración con soluciones CMDB por webservices	2	0
Disponible en entorno web	2	2
Sub total	**18**	**20**
Total general	**210**	**212**

8. ANALISIS COMPARATIVO DE COSTO-BENEFICIO:

El costo aproximado las soluciones de descubrimiento de infraestructura tecnológica y Patch Management con System Center de es de S/ 6,100,000.00 soles por 3 años (Incluido IGV).

El costo aproximado las soluciones de descubrimiento de infraestructura tecnológica y Patch Management con Manage Engine es de S/ 6,326,095.05 soles con soporte a 3 años (Incluido IGV).

9. Conclusiones:

De acuerdo con las comparaciones y evaluaciones realizadas en los puntos anteriores, se tienen las siguientes conclusiones:

- En conclusión, se recomienda adquirir las soluciones de descubrimiento de infraestructura tecnológica de las marcas que obtuvieron un puntaje mayor o igual a 44 y Patch Management de las marcas que obtuvieron un puntaje mayor o igual a 148. En ese sentido, ambas alternativas cumplen con las características mínimas necesarias.
- Los costos las soluciones de descubrimiento de infraestructura tecnológica y Patch Management de las marcas evaluadas son referenciales.

Anexo I: PARQUE INFORMÁTICO

La solución ofertada debe cubrir el total de equipos informáticos, las cantidades son referenciales y deben considerar un crecimiento del 20% anual.

Parque Informático	Cantidad
Servidores físicos	162
Servidores virtuales	2762
PC	17,167
Switches	750
Impresoras	829
Firewall	131
Router	324 (en modalidad comodato)
Access point	496
proyectores	370
Teléfonos IP	5,826
Tablets	126
Equipos móviles	4498
Cámaras IP	403