



**ACTA DE LA JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL PRESENCIAL PARA LA “ADQUISICIÓN DE EQUIPO DE LABORATORIO,
CÓMPUTO Y SOFTWARE DEL PROGRAMA DE FORTALECIMIENTO DE LA CALIDAD EDUCATIVA 2019”.**

**No. Asignado por Compranet: LA-916066971-E5-2019.
No. de Control Interno: UMSNH/LPN/A03-2019.**

En la Ciudad de Morelia, Michoacán siendo las 9:00 horas, del día 09 de octubre del 2019, en la Sala de Prensa del Centro de Información, Arte y Cultura (CIAC) de la Universidad Michoacana de San Nicolás de Hidalgo, con domicilio en Avenida Francisco J. Mújica S/N, colonia Díaz Ordaz, C.P. 58000, se reunieron los servidores universitarios y licitantes, cuyos nombres y firmas aparecen al final de la presente acta, con objetivo de llevar a cabo la Junta de Aclaraciones a la Convocatoria de la Licitación Pública Nacional Presencial, que se realiza para la “Adquisición de Equipo de Laboratorio, Cómputo y Software del Programa de Fortalecimiento de la Calidad Educativa 2019”, No. Asignado por Compranet: LA916066971-E5-2019, y No. de Control Interno: UMSNH/LPN/A03-2019. Acto que se realiza conforme a lo establecido a los artículos 33 y 33 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), 45 y 46 del Reglamento de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público (RLAASSP), así como en el punto número VII de las bases correspondientes.

Este acto fue presidido por la **M.E. en M.F. Silvia Hernández Capi**, Presidente del Comité, quién realizó la presentación de los integrantes del Comité y/o de sus representantes, cuyos nombres y cargos aparecen a final de esta acta.

Posteriormente, verificó la asistencia de los licitantes que en términos del artículo 45 del RLAASSP, se registraron y presentaron el escrito de interés para participar en la licitación, siendo los siguientes:

LICITANTES
ONDACELL, S.A. DE C.V.
SERVERWARE, S.A. DE C.V.
MULTISISTEMAS VALCER, S.A. DE C.V.
CONSORCIO CIENTIFICO DEL BAJÍO, S.A. DE C.V.
MRD CONVERGENCIA TECNOLOGICA, S.A. DE C.V.

El Presidente del acto, señaló que conforme a lo establecido en el artículo 33 bis de la LAASSP, "LA CONVOCANTE" sería asistido, en este acto por los servidores universitarios, cuyos nombres se señalan al final de esta acta, quienes representan al área requirente y/o área técnica, y acuden al presente acto para resolver en forma clara y precisa las dudas y planteamientos de los licitantes relacionados con los aspectos contenidos en la Convocatoria.

El presidente del acto indicó que previo a dar respuesta a las solicitudes de aclaración recibidas, era necesario realizar la siguiente aclaración, por parte de "LA CONVOCANTE":

1. EL DÍA 03 DE OCTUBRE DEL PRESENTE AÑO, SE PÚBLICO EN EL DIARIO OFICIAL DE LA FEDERACIÓN LA CONVOCATORIA A LA LICITACIÓN PÚBLICA NACIONAL PRESENCIAL PARA LA "ADQUISICIÓN DE EQUIPO DE LABORATORIO, CÓMPUTO Y SOFTWARE PARA EL PROGRAMA DE FORTALECIMIENTO DE LA CALIDAD EDUCATIVA 2019", SEÑALANDO COMO FECHA PARA LA NOTIFICACIÓN DE FALLO EL DÍA VIERNES 23 DE OCTUBRE DEL 2019, SIENDO QUE EL DÍA CORRECTO PARA DICHO ACTO ES EL DÍA MIÉRCOLES 23 DE OCTUBRE DEL 2019 A LAS 12:00 DEL DÍA.
2. REFERENTE A LAS PARTIDAS 12, 13, 15, 53, 54, 55 y 55, DEBERÁN CONSIDERARSE LAS CARACTERÍSTICAS COMPLEMENTARIAS QUE EL ÁREA REQUIRENTE HIZO LLEGAR, LAS CUALES FORMARÁN PARTE DE LA PRESENTE ACTA.
3. EN LAS BASES EMETIDAS POR "LA CONVOCANTE, EN EL PUNTO TERCERO, INCISO V), DENOMINADO "DEMORAS Y PENAS CONVENCIONALES", SE INDICO QUE EN EL CASO DE QUE LOS BIENES NO SEAN ENTREGADOS DENTRO DEL PLAZO SEÑALADO, "EL PROVEEDOR", QUEDARÁ OBLIGADO A PAGAR A "LA UNIVERSIDAD", POR CADA DÍA DE RETRASO UNA PENA CONVENCIONAL EQUIVALENTE DEL 10% (DIEZ POR CIENTO), DEBIÉNDOSE INDICAR QUE LA PENA CONVENCIONAL DEBERÁ DE SER DEL 1% (UNO POR CIENTO) AL 10 % (DIEZ POR CIENTO) POR CADA DÍA DE RETRASO.

Posteriormente, el Presidente del acto precisó que conforme a lo establecido en el artículo 45 del RLAASSP, **únicamente se dará respuesta a las solicitudes de aclaración que hayan sido presentadas en tiempo y forma, y que hayan sido planteadas de manera concisa y que estén directamente vinculadas con los puntos contenidos en la Convocatoria a las Licitación Pública Nacional Presencial**, indicando el numeral o punto específico con el cual se relaciona; por lo que las solicitudes que no cumplan con los requisitos, serán desechadas por "LA CONVOCANTE".

Se informó que las solicitudes de aclaración recibidas, en tiempo y forma, fueron las siguientes:

A) MRD CONVERGENCIA TECNOLÓGICA, S.A. DE C.V.

PREGUNTAS ADMINISTRATIVAS

1. Inciso III punto v; menciona **Demoras y penas convencionales**: En caso de que los bienes no sean entregados dentro del plazo señalado, "EL PROVEEDOR", quedará obligado a pagar a "LA UNIVERSIDAD", por cada día de retraso una pena convencional equivalente del **10% (diez por ciento)**, del valor del contrato respectivo. Pregunta el porcentaje mencionado es incorrecto, ¿qué porcentaje se aplica?

Respuesta: Ya fue aclarado por "LA CONVOCANTE."

2. Inciso VIII, **Acto y Presentación de Proposiciones**, punto No. d, Garantía de seriedad de las proposiciones por el importe máximo. En el párrafo tercero menciona "Esta garantía permanece en custodia de "LA CONVOCANTE", una vez transcurridos 15 días hábiles posteriores al fallo, tiempo en el que será entregada a los licitantes mediante solicitud escrita, salvo la de aquel a quien se adjudique el contrato, la cual será canjeada por la garantía de cumplimiento de contrato. **(FORMATO K).**" Pregunta ¿El formato K mencionado aplica para la garantía de seriedad cuando es fianza, en el caso de garantizar con cheque de caja este se anexa a un formato libre, es correcto?

Respuesta: Es correcto.

PREGUNTAS TÉCNICAS

3. Partida 10, solicitan impresora con **soporte experto de por vida**, por el tiempo tan corto que hay desde la publicación de las bases y él envió de las preguntas, aun no recibimos respuesta por parte del fabricante respecto a la cobertura de soporte, preguntamos al usuario, ¿En caso de que dicho soporte tenga costo adicional, tienen contemplado este costo en su presupuesto o en su defecto si representa un incremento en el precio omitimos el soporte?

Respuesta: El soporte experto de por vida va incluido dentro del precio de la compra. Y se refiere a la asesoría para el funcionamiento de la impresora, así como a la utilización de la misma. No incluye mantenimiento o reparación de la impresora. Por lo que consideramos no omitir el soporte de por vida en la licitación.

4. Partida 30, 31 y 32, solicitan equipo de cómputo, ¿Solicitamos a la dependencia nos especifique de qué tamaño requiere el procesador del equipo?

Respuesta: Mínimo 1.7 GHZ

5. Partida 33, solicitan memorias, en las cuales mencionan dos números de parte diferente, ¿favor de especificar que memoria requieren o si requieren se coticen las dos como un único precio a ofertar?

Respuesta: Se dan dos números de parte diferente porque cualquiera es compatible. Si se debe elegir cotizar AD3U1600W4G11-S.

6. Partida 33, solicitan memoria con una latencia CAS CL9, uno de los números de parte mencionados tiene un CL=11, ¿se acepta?

Respuesta: Se acepta.

7. Partida 34, solicitan velocidad de escritura de 430 MB/s, pero la hoja de datos del fabricante no lo menciona la velocidad de escritura, se solicita que se omita esta característica en la descripción.

Respuesta: Se acepta.

8. Partida 35, Solicitan servidor, sin embargo, la descripción refiere a una Workstation, además la descripción del modelo solicitado se encuentra descontinuado por el fabricante, por lo anterior solicitamos nos especifiquen si requieren una Workstation o un Servidor, y nos permitan ofertar equipo de iguales o superiores características de la misma u otra marca ¿Se acepta?

Respuesta: Se requiere workstation y se permite ofertar de la misma marca u otras con superiores características (se acepta).

9. Partida 40, solicitan doble batería recargable de ION-Litio NB-11L, pero el empaque solo contiene 1, Debemos entender que requieren dos empaques por cada precio ofertado, ¿Es correcta nuestra apreciación?

Respuesta: En efecto, se necesitan por cada cámara dos baterías.

10. Partida 57, solicitan licencia de software para controlar el sistema térmico de sistemas operativos, solicitamos al usuario especificar marca y versión del software que necesitan.

Respuesta: Marca: Macs Fan Control Pro, version 1.5

11. Partida 60, Por el requerimiento de esta partida al ser productos integrales es imprescindible el apoyo del fabricante, por su alcance y ser una solución llave en mano, ¿se requiere carta de apoyo del fabricante?

Respuesta: Es necesario, la presentación de la carta de apoyo del fabricante.

B) MULTISISTEMAS VALCER, S.A. DE C.V.

PREGUNTAS ADMINISTRATIVAS

1. En las bases de ésta licitación, no se solicita presentar Declaración Anual de ejercicio fiscal anterior (2018) y la declaración de pagos provisionales de impuestos federales del mes de septiembre 2019. ¿Es imperativo presentar estos documentos en nuestra propuesta técnica?

Respuesta: Es necesario la presentación de ambos documentos.

2. Existen situaciones en donde el proceso de licitación después de la presentación de las propuestas técnicas, alguno o algunos de los productos son descontinuados por el fabricante y remplazados por otros.

Si este fuera el caso, ¿podemos entregar un producto de mayor o iguales especificaciones técnicas a las ofertadas?

Respuesta: Se acepta.

3. ¿Para todas las partidas involucradas en esta licitación debemos hacer mención de las marcas, modelos, y números de parte de los productos contemplados en cada partida solicitada?

Respuesta: Es correcto.

4. Observamos que algunas de las partidas que corresponden al anexo técnico de ésta licitación están incompletas; ejemplo: partidas 53, 54 y 55, hace falta más información de carácter técnico. ¿Nos podrían facilitar la información completa?

Respuesta: Ya fue aclarada por "LA CONVOCANTE".

5. ¿Debemos entender que para ésta licitación no se debe presentar ninguna carta de apoyo de por parte de mayoristas para ésta Licitación?

Respuesta: Es necesario se presenten para las partidas ofertadas las cartas de apoyo correspondientes.

C) SERVER WARE, S.A. DE C.V.

PREGUNTAS TÉCNICAS

1. Se le solicita a la Convocante, pueda aclarar el requerimiento sobre la Partida No. 51:

1.1.1.9 VEINTE (20) DISCOS DUROS HPE (NUEVOS EN CAJA SELLADA, NO REACONDICIONADOS) DE 2TB EXACTOS DE CAPACIDAD 6GB SAS 3.5" LFF PARA SISTEMA DE ALMACENAMIENTO HPE 3PAR STORSERV 7200 7400 QUE INCLUYEN EL MICRO-CÓDIGO (FIRMWARE) MÍNIMO Y NECESARIO PARA SU ADMISIÓN EN CALIENTE AL SISTEMA DE ALMACENAMIENTO Y QUE ADEMÁS INCLUYA LA MEDIA DE INSTALACIÓN CON LAS ACTUALIZACIONES DE SOFTWARE REQUERIDAS HASTA LA VERSIÓN 3PAR INFORM OS RELEASE 3.3.1 MU2 P90.

- Si se tiene el espacio o chasis para integrar los 20 Discos de 3.5".

Respuesta: Si se cuenta con el espacio para instalar los discos.

- Si nos puede indicar que los discos que se tienen actualmente tienen encriptación de datos ó no.

Respuesta: No se requiere la encriptación.

- Conocer el nivel de licenciamiento que se tiene en los Discos.

Respuesta: Si se cuenta con licenciamiento para los discos.

- Por favor indicar si serán necesarios servicios customizados de rebalanceo y configuración de la nueva infraestructura.

Respuesta: No se requieren los servicios mencionados, únicamente la medida de instalación con las actualizaciones de software requeridas hasta la versión 3PAR INFORM OS RELEASE 3.3.1 MU2 P90.

- Si nos pueden proporcionar los Números de Parte que se tienen en su infraestructura, esto ya que es necesario considerar el crecimiento que se solicita y los servicios e infraestructura que se necesitan para la instalación y rebalanceo de la solución.

Respuesta: Los números de parte son: QR482A, QR491A

2. Se le solicita a la Convocante, pueda aclarar el requerimiento sobre la Partida No. 52:

DOS (2) HPE 3PAR PHYSICAL SERVICE PROCESSORS DL320E GEN8 V2 E3-1220V3 PARA SERVICIO REDUNDANTE CON LA MEDIA DE INSTALACIÓN DE LAS VERSIONES DE SOFTWARE PARA INSTALAR SP-4.4.0.GA-129 (MU8), INTERIM SP-4.5.0 (MU4) Y SP- 5.0.5.1-27035 (MU5) CON SOPORTE PARA ACTUALIZAR UN EQUIPO HPE STORESERV. FUNCIÓN DE RECOPIACIÓN DE DATOS DEL SISTEMA DE ALMACENAMIENTO DEL HPE 3PAR STORESERV CONECTADO EN INTERVALOS PREDEFINIDOS, ASÍ COMO BAJO DEMANDA, Y ENVIÓ DE LOS DATOS A HEWLETT PACKARD ENTERPRISE.

- Cuál es el Chasis si es 7200 o 7400 que se tiene, para evaluar el Service Processor que debe ser integrado a la solución.

Respuesta: Es un chasis 7200

- El equipo DL320 es un servidor discontinuado por el fabricante, y las opciones certificadas por el fabricante para el service procesor son 2:

- a) Físico HPE 3PAR StoreServ 7000 Service Processor.
- b) Virtual Service Procesor sobre VMWare y Hyper-V.

- Favor de indicar que opción es la que requieren.

Respuesta: Se requiere la opción física

- Favor de indicar si requieren instalación y configuración.

Respuesta: No se requiere instalación ni configuración, únicamente la medida de instalación de las versiones de software para instalar SP-4.4.0GA-129 (MU4) y SP-5.0.5.1-27035 (MU5)

- Favor de indicar el nivel de soporte requerido.

Respuesta: No se requiere ningún nivel de soporte.

Una vez que "LA CONVOCANTE" terminó de dar respuesta a las solicitudes de aclaración, se dio oportunidad a los licitantes para que formularan las preguntas que estimaran pertinentes en relación con las respuestas dadas con anterioridad.

Se dio la palabra a la Apoderada Legal de la Empresa Mrd Convergencia Tecnológica, S.A. de C.V., Arely del Carmen Verduzco Villafuerte, quien señaló que por un error de dedo en la pregunta No. 5 se refería al tamaño de monitor y no al procesador. Asimismo, por parte de "LA CONVOCANTE", se indicó que el tamaño del monitor deberá de ser de 21 pulgadas o superior a este.

Posteriormente, por parte de la Empresa Multisisistemas Valcer, S.A. de C.V., solicito a "LA CONVOCANTE", se pudiera aceptar en el acto de apertura como Garantía de Seriedad una Fianza superior al monto total antes del impuesto del valor agregado de la propuesta económica, a lo que "LA CONVOCANTE", dio su consentimiento.

Al no existir más cuestionamientos, se informó que el contenido de la presente acta formará parte integral de la Convocatoria, y que deberá ser considerada por los licitantes en la elaboración de sus proposiciones; asimismo, se indicó que no habrá otra junta de aclaraciones y que el acto de presentación y apertura de propuesta, se realizará el 14 de octubre del 2019, conforme al calendario de actos establecidos en la Convocatoria respectiva.

Siendo las 09:30 (nueve) horas con (treinta minutos), se dio por concluida la junta de aclaraciones, firmando la presente acta, los que en ella intervinieron y así desearon hacerlo.





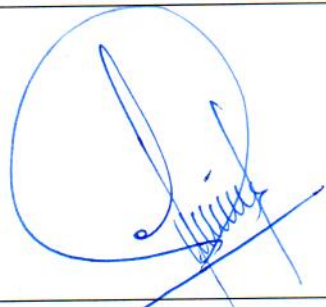
ASISTENTES

SERVIDORES UNIVERSITARIOS

Integrantes del Comité de Adquisiciones, Arrendamientos y Servicios.

M.E. en M.F. Silvia Hernández Capi

Presidente del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.

<p>Lic. José Felipe Álvarez Andrade Representante del Dr. Rodrigo Gómez Mongue, Tesorero de la Universidad y Primer Vocal del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.</p>	
<p>C.P. César Castro Peña Director de Adquisiciones de Bienes y Servicios de la Universidad, y Segundo Vocal del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.</p>	
<p>M. en C. Rodrigo Tavera Ochoa Contralor de la Universidad y Primer Vocal Asesor del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.</p>	
<p>Lic. Luis Fernando Rodríguez Vera Abogado General y Segundo Vocal Asesor del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.</p>	
<p>M.G.A.P. Berenice Álvarez Álvarez Representante del Dr. Adrián Zaragoza Tapia Director de Patrimonio de la Universidad y Tercer Vocal Asesor del Comité de Adquisiciones, Contratación de Servicios y Arrendamiento de Bienes Muebles e Inmuebles de la Universidad Michoacana de San Nicolás de Hidalgo.</p>	

ÁREA REQUERENTE Y TÉCNICA

ÁREA REQUERENTE Y TÉCNICA	
NOMBRE	FIRMA
GILDARDO SOLORIO DÍAZ	



FLORENCIO MOISÉS GONZÁLEZ VALDEZ	
SERGIO MAURICIO ESCOBEDO TORRES	
SONIA ELIZABETH HUERTA AYALA	
OLIVER MAURICIO LÓPEZ GARNICA	
ESPERANZA MELÉNDEZ HERRERA	
JESUS ARMANDO VARGAS CORREA	
CHADAY GISELL ARREGUIN GUERRERO	





REGISTRO DE ASISTENTES


LICITANTES		
LICITANTE	PERSONA QUE ASISTE	FIRMA













ONDACELL, S.A. DE C.V.	RAÚL ARREGUIN LÓPEZ	
SERVERWARE, S.A. DE C.V.	JAVIER MARTÍN CORELLA GARCÉN	
MULTISISTEMAS VALCER, S.A. DE C.V.	VICTOR MANUEL MORA CERCADO	
CONSORCIO CIENTIFICO DEL BAJÍO, S.A. DE C.V.	YOLANDA DURAN TEJEDA	
MRD CONVERGENCIA TECNOLÓGICA, S.A. DE C.V.	ARELY DEL CARMEN VERDUZCO VILLAFUERTE	























Sistema de Procesamiento en High Performance Computing integrado con los siguientes componentes:

Cinco (5) Nodos / Servidores Oracle SPARC Enterprise T4-1 de 2U de rack con las siguientes características:

Procesador Oracle SPARC T4 de 8 núcleos (cores) a 2.85GHz con 8 hilos (threads) de procesamiento por núcleo para un total de 64 hilos de procesamiento simultáneo, 8 unidades de procesamiento de punto flotante, aceleradores de instrucciones de cifrado en el chip con soporte directo no privilegiado para 16 estándares industriales de algoritmos criptográficos, más generación de números aleatorios en cada uno de los ocho núcleos: AES, Camelia, CRC32c, DES, 3DES, DH, DSA, ECC, Kasumi, MD5, RSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 y conjunto de instrucciones fuera-de-orden (out-of-order) SPARC v9.

64 GB de Memoria RAM, soporte máximo de 512 GB.

Interfaz de red de 4 x 1Gb (10/100/1000Mbps) integrada.

Dos slots opcionales para 10GbE XAUI y seis slots PCIe.

Cuatro puertos externos USB y un puerto VGA.

Cuatro discos duros de 600GB a 10000 rpm formato 2.5-inch conexión SAS.

Dos tarjetas de almacenamiento de estado sólido Oracle Sun Flash Accelerator PCIe de 96GB con un desempeño en lectura aleatoria (4K) de 101K IOPS, en escritura aleatoria (4K) 88K IOPS, lectura secuencial (1M) 1.1 GB/seg, escritura secuencial (1M) 567 MB/seg, IO service time (latencia +4K transfer) 0.22 ms, Solid-state NAND Enterprise SLC, MTBF de más de 2M horas, consumo eléctrico de 16.5 Watts.

Unidad de DVD interna slim line SATA DVD+/- RW

Dos fuentes de poder redundantes (1+1) intercambiables en caliente (hot-swappable) de 1200W AC, voltaje de operación 200 to 240 VAC o 100 a 120 VAC, 50/60 Hz

Capacidades de RAS requeridas: Unidades de disco conectables en caliente; Fuentes de alimentación y ventiladores redundantes intercambiables en caliente; Monitoreo ambiental; ECC ampliado, corrección de errores y memoria de comprobación de paridad; Fácil reemplazo de componentes; controlador de disco integrado con RAID 0, 1 y 1E

Capacidades de Gestión Remota requeridas: Oracle Integrated Lights Out Manager (ILOM); Un puerto de administración Ethernet dedicado 10/100base-T; Acceso a la administración de red en banda, fuera de banda y de banda lateral a través de cualquiera de los cuatro principales Puertos Ethernet del servidor; Un puerto de administración serie RJ-45; Interfaz de línea de comandos estilo DTMF; Soporte para acceso a través de SSH 2.0, HTTPS, RADIUS, LDAP y Microsoft Active Directory, GUI basada en navegador para el control del sistema a través de una interfaz gráfica; IPMI 2.0, SNMP v1, v2c y v3; Administración remota con redireccionamiento completo de teclado, video, mouse, almacenamiento (KVMS) y control remoto con capacidad de medios (disquete, DVD, CD y más); Capacidad de supervisar e informar el estado del sistema y los componentes en todas las FRU

Debe incorporar como mínimo el sistema operativo Oracle Solaris 11.4.11.4.0, así como también el firmware del servidor debe estar actualizado como mínimo a la versión 8.9.8 para aceptar las Oracle Solaris Kernel Zones en Oracle Solaris 11.4.

Tres (3) Nodos / Servidores Oracle Sun Server X4-2 de 1U de rack con las siguientes características:

Dos Procesadores Intel Xeon E5-2609 a 2.5GHz con 10 MB SmartCache y potencia de diseño térmico (TDP) de 80 watts.

32 GB de Memoria RAM, soporte máximo de 512 GB.

4 Interfaces de red de 10G (100/1000/10G Base-T) integradas.

Seis puertos externos USB, un puerto VGA y cuatro slots PCIe.

Seis discos duros de 300GB formato 2.5-inch. Fuentes de poder redundantes con 91% de eficiencia.

Capacidades de Gestión Remota requeridas: Oracle Integrated Lights Out Manager (ILOM); Un puerto de administración Ethernet dedicado 10/100base-T; Acceso a la administración de red en banda, fuera de banda y de banda lateral a través de cualquiera de los cuatro principales Puertos Ethernet del servidor; Un puerto de administración serie RJ-45; Interfaz de línea de comandos estilo DTMF; Soporte para acceso a través de SSH 2.0, HTTPS, RADIUS, LDAP y Microsoft Active Directory, GUI basada en navegador para el control del sistema a través de una interfaz gráfica; IPMI 2.0, SNMP v1, v2c y v3; Administración remota con redireccionamiento completo de teclado, video, mouse, almacenamiento (KVMS) y control remoto con capacidad de medios (disquete, DVD, CD y más); Capacidad de supervisar e informar el estado del sistema y los componentes en todas las FRU

Soporta los sistemas operativos Oracle Solaris, Oracle Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows Server, Oracle VM, VMware

Un (1) Conmutador de Red Extreme Networks ExtremeSwitching Summit X440-G2-48p-10GE4 con las siguientes especificaciones:

- 48 x 10/100/1000BASE-T PoE-Plus
- 4 x 1GBASE-X SFP combo ports
- 2 x 1GbE copper combo ports upgradable to 10GbE on rear-panel
- 4 x 1GBASE-X SFP (unpopulated rear-panel ports) upgradable to 10Gb Ethernet via licensing
- 1 x Serial (console port RJ-45) with RTS/CTS modem control
- 1 x 10/100/1000BASE-T out-of-band management port
- 2x9 RPS port

Dos (2) Fuentes de Poder Delta Electronics Modelo DPS-600SB D REV:00F.

Un (1) Modulo de batería de reemplazo para HPE EVA 4400 460581-001

Dieciséis (16) Transceptores Láser Clase 1 de Fibre Channel (FC) 8G Brocade.

Dos (2) Conmutadores de Red Extreme Networks con 48 puertos Ethernet, 2 puertos 1000BASE-X, Capa 3 con soporte de:

(RIP) RFC 1058 RIPv1, RFC 2453 RIPv2; (OSPF) RFC 2328 OSPFv2, RFC 1587 OSPF NSSA Option, RFC 2154 OSPF with Digital Signatures (password, MD-5); RFC2338 Virtual Redundant Router Protocol (VRRP)

(BGP4) RFC 1771 Border Gateway Protocol 4, RFC 1965 Autonomous System Confederations for BGP, RFC 1966 BGP Route Reflection, RFC 1997 BGP Communities Attribute, RFC 1745 BGP/OSPF interaction;

(IP Multicast) RFC 2362 PIM-SM, PIM-DM Draft IETF PIM Dense Mode v2-dm-03, RFC 1122 DVMRP Host req DVMRP v3 draft IETF DVMRP v3-07, RFC 2236 IGMP v2, IGMP Snooping with configurable router registration forwarding;

(Quality of Service) IEEE 802.1D - 1998 (802.1p) packet priority, RFC 2474 DiffServ Precedence, RFC 2598 DiffServ Expedited Forwarding, RFC 2597 DiffServ Assured Forwarding, RFC 2475 DiffServ Core and Edge router functions;

Un (1) Servidor Oracle SPARC Enterprise T4-1 de 2U de rack con las siguientes características:

Procesador Oracle SPARC T4 de 8 núcleos (cores) a 2.85GHz con 8 hilos (threads) de procesamiento por núcleo para un total de 64 hilos de procesamiento simultáneo, 8 unidades de procesamiento de punto flotante, aceleradores de instrucciones de cifrado en el chip con soporte directo no privilegiado para 16 estándares industriales de algoritmos criptográficos, más generación de números aleatorios en cada uno de los ocho núcleos: AES, Camelia, CRC32c, DES, 3DES, DH, DSA, ECC, Kasumi, MD5, RSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 y conjunto de instrucciones fuera-de-orden (out-of-order) SPARC v9.

64 GB de Memoria RAM, soporte máximo de 512 GB.

Interfaz de red de 4 x 1Gb (10/100/1000Mbps) integrada.

Dos slots opcionales para 10GbE XAUI y seis slots PCIe.

Cuatro puertos externos USB y un puerto VGA.

Cuatro discos duros de 600GB a 10000 rpm formato 2.5-inch conexión SAS.

Dos tarjetas de almacenamiento de estado sólido Oracle Sun Flash Accelerator PCIe de 96GB con un desempeño en lectura aleatoria (4K) de 101K IOPS, en escritura aleatoria (4K) 88K IOPS, lectura secuencial (1M) 1.1 GB/seg, escritura secuencial (1M) 567 MB/seg, IO service time (latencia +4K transfer) 0.22 ms, Solid-state NAND Enterprise SLC, MTBF de más de 2M horas, consumo eléctrico de 16.5 Watts.

Unidad de DVD interna slim line SATA DVD+/- RW

Dos fuentes de poder redundantes (1+1) intercambiables en caliente (hot-swappable) de 1200W AC, voltaje de operación 200 to 240 VAC o 100 a 120 VAC, 50/60 Hz

Capacidades de RAS requeridas: Unidades de disco conectables en caliente; Fuentes de alimentación y ventiladores redundantes intercambiables en caliente; Monitoreo ambiental; ECC ampliado, corrección de errores y memoria de comprobación de paridad; Fácil reemplazo de componentes; controlador de disco integrado con RAID 0, 1 y 1E

Capacidades de Gestión Remota requeridas: Oracle Integrated Lights Out Manager (ILOM); Un puerto de administración Ethernet dedicado 10/100base-T; Acceso a la administración de red en banda, fuera de banda y de banda lateral a través de cualquiera de los cuatro principales Puertos Ethernet del servidor; Un puerto de administración serie RJ-45; Interfaz de línea de comandos estilo DTMF; Soporte para acceso a través de SSH 2.0, HTTPS, RADIUS, LDAP y Microsoft Active Directory, GUI basada en navegador para el control del sistema a través de una interfaz gráfica; IPMI 2.0, SNMP v1, v2c y v3; Administración remota con redireccionamiento completo de teclado, video, mouse, almacenamiento (KVMS) y control remoto con capacidad de medios (disquete, DVD, CD y más); Capacidad de supervisar e informar el estado del sistema y los componentes en todas las FRU

Debe incorporar como mínimo el sistema operativo Oracle Solaris 11.4.11.4.0, así como también el firmware del servidor debe estar actualizado como mínimo a la versión 8.9.8 para aceptar las Oracle Solaris Kernel Zones en Oracle Solaris 11.4, asimismo se incluye el binario de instalación para el servidor de transmisión en formato de streaming por Internet desde Solaris 11.4 con soporte de los codificadores Ogg Vorbis y MP3 de la estación de radio institucional Radio Nicolaita.

Un (1) MicroServidor con procesador Intel de 2.5GHz, conectividad Ethernet 1Gb 2-port, iLO Management Engine, Almacenamiento en Estado Solido en configuración RAID 1 (Mirroring), Tarjeta de Sonido de Alta Fidelidad con soporte de 192kHz/24-bit a 116dB SNR, incluye software para la transmisión de audio en formato de streaming por Internet.

OP/PFCE-2019-16MSU0014T-02-01, BMS 2.1.1.1.10

Un (1) Nodo / Servidor Oracle Sun Server X4-2 de 1U de rack con las siguientes características:

Dos Procesadores Intel Xeon E5-2609 a 2.5GHz con 10 MB SmartCache y potencia de diseño térmico (TDP) de 80 watts.

32 GB de Memoria RAM, soporte máximo de 512 GB.

4 Interfaces de red de 10G (100/1000/10G Base-T) integradas.

Seis puertos externos USB, un puerto VGA y cuatro slots PCIe.

Seis discos duros de 300GB formato 2.5-inch. Fuentes de poder redundantes con 91% de eficiencia.

Capacidades de Gestión Remota requeridas: Oracle Integrated Lights Out Manager (ILOM); Un puerto de administración Ethernet dedicado 10/100base-T; Acceso a la administración de red en banda, fuera de banda y de banda lateral a través de cualquiera de los cuatro principales Puertos Ethernet del servidor; Un puerto de administración serie RJ-45; Interfaz de línea de comandos estilo DTMF; Soporte para acceso a través de SSH 2.0, HTTPS, RADIUS, LDAP y Microsoft Active Directory, GUI basada en navegador para el control del sistema a través de una interfaz gráfica; IPMI 2.0, SNMP v1, v2c y v3; Administración remota con redireccionamiento completo de teclado, video, mouse, almacenamiento (KVMS) y control remoto con capacidad de medios (disquete, DVD, CD y más); Capacidad de supervisar e informar el estado del sistema y los componentes en todas las FRU

Soporta los sistemas operativos Oracle Solaris, Oracle Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows Server, Oracle VM, VMware, asimismo se incluye el binario de instalación para el servidor del servicio de nombres de dominio (DNS) Berkeley Internet Name Domain (BIND) en una versión igual o superior a 9.12.3p4 para SPARC con soporte para delegación de zonas en la nube y para el servidor de tiempo Network Time Protocol (NTP) 4.2.8p11

Dos (2) Nodos / Servidores Oracle SPARC Enterprise T1000

Memoria: 8GB de RAM, Disco Duro: 250GB, Procesador: UltraSPARC T1, Sistema Operativo: Oracle Solaris 11.3.24.4, Fuente de Poder de 300 Watts, ALOM CMT, Hardware-assisted cyptographic acceleration, OpenBoot PROM, Compatible con binarios SPARC® V9, además el firmware del servidor debe incluir/estar actualizado como mínimo a la versión 6.7.13

Servicio de Renovación del Contrato de Licenciamiento Institucional para el Software Antivirus Symantec Endpoint Protection

Incluye Licencias de Antivirus Symantec Endpoint Protection por 2 años para 2500 Equipos de Cómputo Universitarios de acuerdo con las fechas de renovación y vigencia que correspondan a la renovación del certificado #15015038 con las siguientes características:

Requerimientos Generales de la solución:

La solución deberá brindar protección para servidores, equipos portátiles y estaciones de trabajo sobre deberá estar soportado para instalarse en: Sistemas operativos Windows: Windows Vista (32 o 64 bits), Windows 7 (32 o 64 bits), Windows 7 Embedded, Windows 8 (32 o 64 bits), Windows 8 Embedded, Windows 8.1, Windows 10, Windows Server 2003 (32 bits, 64 bits, R2, SP1 o posterior), Windows Server 2019, Mac OS X 10.6.8, 10.7 (32 bits, 64 bits); 10.8 (64 bits), Mac OS X Server 10.6.8, 10.7 (32 bit o 64 bits); 10.8 (64-bit).

Deberá ser capaz de proveer funcionalidad de protección con las siguientes tecnologías

- Antivirus basado en firmas y definiciones
- Motor reputacional alimentado por mecanismos globales de inteligencia
- Motor de detección basado en machine learning incorporado en el motor de detección de la protección Heurística del punto final
- Protección contra amenazas a través de la protección proactiva contra el aprovechamiento de vulnerabilidades como el abuso del Exception Handler y ataques tipo Heap Spray
- Antispyware
- Firewall de Máquina para clientes Windows
- IDS/IPS de punto final
- Motor de detección y prevención contra intrusos
- Control de aplicaciones
- Control de dispositivos
- Control de Integridad
- Motor heurístico basado en comportamiento
- Capacidad de Listas Blancas y negras para control de aplicaciones
- Monitoreo de comportamiento de aplicaciones
- Control físico de dispositivos
- Protección de Integridad de la Máquina
- Reportes avanzados.
- Borrado seguro de malware residente en memoria difíciles de erradicar, para evitar el reinicio de servidores críticos.

La solución deberá estar listada en el último cuadrante mágico de Gartner para protección del punto final y deberá aparecer como uno de los líderes de dicho cuadrante.

La solución deberá permitir que el uso e integración de las tecnologías de protección sea a través de políticas configurables y flexibles en un esquema jerárquico (dominios, sitios, grupos, subgrupo, cliente, usuario, localidades, etc.) para aplicar a perfiles de usuario o equipos en base a los criterios definidos por la institución y deberán asignarse desde la consola de administración de la solución.

La solución de protección deberá ser configurable para definir de forma flexible diferentes niveles de interacción con el usuario final, es decir permitir al usuario realizar algunas o varias funciones o restringirlas por completo.

La solución de protección deberá permitir que las actualizaciones llámese versiones, parches, adecuaciones o modificaciones propias de la solución de protección puedan realizarse de forma automatizada con escasa o nula interacción administrativa teniendo en cuenta un parque de equipos protegidos de la institución es de al menos 2500 estaciones de trabajo (Servidores y Computadores Personales). Se debe presentar carta de apoyo por parte de Symantec de México

La solución deberá ser capaz de prevenir la desinstalación sin autorización de la herramienta e incluso poder utilizar una contraseña.

La solución deberá ser capaz de evitar que los procesos correspondientes que proveen la protección sean manipulados, deshabilitados o comprometidos en forma mal intencionada o sin autorización.

La solución deberá ser capaz de enviar en forma automática al fabricante los riesgos de seguridad detectados para su revisión y valoración.

La solución deberá poder desinstalar la solución de antivirus existente antes de hacer la instalación del nuevo antivirus.

La solución deberá permitir la configuración flexible de acciones a tomar ante la detección de riesgos de seguridad.

La solución deberá ser capaz de configurar notificaciones sobre la detección de riesgos en base a roles o perfiles de responsabilidad definidos por la entidad.

La solución deberá ser capaz de soportar esquemas de replicación, balanceo de cargas en las consolas de administración centralizadas para estar abiertos a la implementación de planes de recuperación de desastres y disponibilidad de servicio.

La solución deberá ser capaz de integrarse al directorio activo para importar y configurar estructuras organizacionales (usuarios y equipos) para ser cubiertos con la protección de seguridad.

La solución debe ser capaz de manejar diferentes formas de instalación en los equipos de los usuarios finales (por ejemplo, interactiva, silenciosa, reiniciar equipo o no).

La solución deberá contar con el respaldo de una base de datos de conocimientos, descargas, actualizaciones, documentación, soporte, seguimientos de casos de escalación, despliegue de información provista y mantenida directamente por el fabricante.

La solución deberá ser capaz de manejar un esquema que incluya cuarentena centralizada de los riesgos de seguridad detectados.

La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales administrados centralmente como a usuarios finales que descentralizados.

La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales como a servidores de propósito específico.

La solución deberá ser capaz de soportar la administración centralizada de un ambiente de mínimo ##### usuarios finales.

La solución deberá ser capaz de soportar el uso de BDs externas (no propietarias de la solución) por ejemplo SQL server.

La tecnología de protección provista por la solución deberá ser altamente efectiva para la detección y remoción de riesgos de seguridad en la categoría de rootkits.

La solución incorporará un motor de remoción para amenazas incluyendo la programación de reinicios para remover completamente las amenazas.

La instalación del agente de protección deberá poder realizarse de al menos los siguientes métodos: local utilizando la media de instalación, remotamente desde la consola, por medio de un servidor de Intranet o utilizando herramientas de distribución de terceros.

La comunicación del agente con la consola de administración deberá poder realizarse por medio de los protocolos http y https para facilitar la inspección de tráfico y evitar la apertura de puertos en firewalls y otros dispositivos de red.

La solución deberá actualizar su contenido (firmas de detección de virus, firmas de detección de intrusos, listado de aplicaciones) desde la consola de administración, desde Internet, desde un equipo definido para la actualización local, inclusive en forma manual.

La solución de protección deberá incluir tecnología de antivirus y antispyware que detecte intentos de infección desde unidades de disco, unidades removibles, unidades compartidas, así como memoria.

La solución de protección podrá ser configurada para que al intentar abrir la interface del usuario solicite una contraseña, en caso de no conocer la contraseña, el usuario no podrá abrir la interface.

Las políticas para la solución de protección deberán poderse aplicar por computadora o por usuario, deberán poderse aplicar por grupo, subgrupo o a todo el universo de equipos.

La solución de protección deberá tener capacidad para identificar el tipo de red al cual se está conectando para adecuar las políticas de protección de antivirus y antispyware, Firewall, IPS, control de Dispositivos, así como de políticas de actualización. La detección de la ubicación deberá poder realizarse por al menos las siguientes variables: rango de dirección IP, dirección IP/nombre del servidor de nombres DNS, dirección IP/nombre del servidor de WINS, default Gateway.

Administración:

Deberá contar con una consola de administración centralizada, desde la cual se pueda monitorear el estado de la seguridad en los equipos de cómputo de la institución.

La consola deberá tener la capacidad de ser accedida desde cualquier punto de la red utilizando un navegador de páginas de Internet como Internet Explorer o Mozilla Firefox.

La consola de administración deberá mostrar en una gráfica el estado de la actualización de los patrones de detección en los agentes. En una tabla de mayor detalle deberá indicar el nombre del equipo, su dirección IP, el usuario que se firmó en el equipo y el sistema operativo.

La consola de administración deberá mostrar en una gráfica los intentos de infección más recientes, así como los equipos que presentaron dichos intentos de infección indicando además la acción tomada por el agente de protección.

La consola de administración deberá mostrar un indicativo del estado de la seguridad en Internet, este estado deberá permitir al administrador de la solución identificar los niveles de riesgo del exterior para poder realizar ajustes en las políticas de protección.

La consola de administración deberá funcionar como un repositorio central de políticas para las tecnologías de Antivirus, firewall personal, detección y prevención de intrusos, así como de protección al sistema operativo y control de dispositivos.

La consola de administración deberá contar con un esquema de autenticación local, con enlace al directorio activo o con un enlace por medio de RSA para autenticación fuerte

La consola de administración deberá permitir la creación de administración por roles, para permitir la institución una segregación de funciones.

La consola de administración deberá permitir la generación de reportes gráficos que permitan identificar: los intentos de infección más repetidos en el ambiente de la institución, los equipos con mayor número intentos de infección, versión del agente de protección instalado en los equipos y un reporte de los equipos con las firmas de contenido.

La consola de administración deberá integrar una función que permita reconocer equipos que no tengan el agente de protección instalado. Para posteriormente enviárselo a través de la consola.

La consola de administración deberá permitir la instalación remota del agente de protección en los equipos que no cuenten con dicho software. La instalación deberá poderse realizar dando el nombre del equipo, su dirección IP o una lista combinando ambas opciones.

La consola de administración deberá permitir la creación de roles para definir diferentes niveles de administración.

La herramienta debe poder aplicar diferentes políticas a los equipos clientes, de acuerdo a la ubicación de los mismos. Esta ubicación se podrá definir de acuerdo al tipo de conexión (ethernet, ethernet, vpn, dial-up), rango de IP, DNS, entre otros.

El motor de detección de Intrusos (IDS) permitirá la creación de firmas de detección de red para bloquear o monitorear el tráfico de red de aplicaciones.

Características de la tecnología antivirus:

La tecnología de antivirus deberá contar con certificación AV-Test Corporativa más actual y deberá contactar con la certificación AAA de SELabs.

La tecnología de antivirus de la solución deberá ser capaz de detectar y eliminar spyware.

La tecnología de antivirus de la solución deberá ser capaz de analizar los mensajes de correo electrónico recibidos en los protocolos SMTP (Simple Mail Transfer Protocol) y POP3 (Post Office Protocol).

La tecnología antivirus de la solución deberá poder actualizar sus definiciones de virus desde Internet, el servidor central y desde un repositorio local (será decisión de la institución determinar el método más adecuado teniendo en cuenta diversos factores), la actualización de definiciones deberá poderse programar para realizarse en un horario que no provoque afectación a la red.

La tecnología antivirus de la solución deberá ser capaz de realizar las actualizaciones de forma óptima, firmas de virus, así como el motor de búsqueda (por ejemplo, utilizando actualizaciones diferenciales y métodos de distribución).

La tecnología antivirus de la solución deberá ser capaz de analizar archivos comprimidos en al menos los siguientes formatos: ZIP, RAR, y TAR con capacidad de analizar hasta 10 niveles de compresión.

La tecnología de antivirus de la solución deberá ser capaz de definir exclusiones por tipo de archivo, directorios y tipo de amenaza.

La tecnología de antivirus deberá realizar escaneos de los equipos de manera eficiente, excluyendo todos aquellos archivos que, basados en reputación por parte del fabricante, no representen un riesgo, al contar con una buena reputación.

Las políticas de antivirus de la solución deberán poderse adaptar de acuerdo al reconocimiento de la red a la cual se está conectando.

El fabricante de la solución deberá tener su propio centro de investigación y respuesta de virus, además debe poder generar actualización a contenidos para las tecnologías de antivirus, el firewall personal y detección y prevención de intrusos.

La tecnología de antivirus deberá contar con tecnología de reputación, es decir que valide si un archivo goza de mala reputación para que este sea bloqueado, o si goza de buena reputación para que este sea excluido.

El agente deberá ofrecer protección al descargar archivos desde internet, al validar que el archivo descargado tenga una reputación aceptable, o en términos de distribución y antigüedad del mismo a nivel mundial.

La solución deberá contar con herramientas con permitan escáner máquinas virtuales off-line.

La solución deberá contar con la capacidad de excluir en las máquinas virtuales, todos aquellos archivos que ya hayan sido escaneados de una imagen base, con la finalidad de reducir el consumo de recursos.

Características de la tecnología de firewall personal y prevención de intrusos:

La tecnología de firewall personal de la solución deberá ser de tipo stateful inspection capaz de analizar el tráfico en paquetes de tipo TCP, UDP, ICMP, ICMPv6, IP y en flujo de datos.

La tecnología de firewall deberá permitir soportar los protocolos IP, TCP, UDP, ICMP, ICMPv6, IP y Ethernet y crear reglas basados en dichos protocolos.

La tecnología de firewall deberá permitir soportar del protocolo IP los tipos: ICMP, IGMP, GGP y otros para ser especificados en las reglas del firewall.

La tecnología de firewall de la solución deberá permitir la definición de reglas por aplicación, por protocolo, por horario, por dirección IP y por tipo de tarjeta de red.

La tecnología de firewall de la solución deberá integrar un módulo de detección y prevención de intrusos, deberá contener firmas de ataques, estas firmas deberán ser actualizadas desde Internet o desde el servidor central. El fabricante deberá especificar documentación de las firmas de protección contra intrusos integradas.

La tecnología de firewall de la solución deberá contener un módulo que permita el reconocimiento de explotación de vulnerabilidades no importando el método de explotación que se esté utilizando.

Firewall de punto final con soporte para IPv4 y IPv6. Dicho firewall estará soportado para máquinas servidores Windows 2008 R2 y posterior.

La tecnología de firewall de la solución deberá tener un módulo de inspección profunda para los protocolos DHCP, DNS y WINS.

La tecnología de firewall de la solución deberá ser capaz de configurar el navegador en modo seguro de tal manera que no publique la versión del navegador.

La tecnología de firewall de la solución deberá ser capaz de detectar y bloquear ataques de OS fingerprint y de generación de secuencias de TCP.

La tecnología de detección de intrusos de la solución deberá incluir ataques en diferentes categorías, las categorías incluidas deberán ser: ataques de buffer overflow, puertas traseras, ataques de negación de servicios, puertas traseras, programas de P2P, mensajeros y propagación de amenazas.

La tecnología de antivirus deberá contar un módulo de evaluación de posturas de seguridad, considerando al menos búsqueda de llaves de registro, estado de antivirus, la presencia de un archivo e inclusive ejecutar scripts y contar con una serie de respuestas en caso de ser necesario, desde el mismo software de antivirus, sin instalar un software adicional en los clientes o consola de administración adicional.

La tecnología de detección de intrusos también se deberá integrar al navegador de internet, para brindar protección a los usuarios finales.

Características de control de integridad:

La tecnología de análisis de integridad deberá poder identificar parches de sistema operativo instalados, software de terceros de seguridad instalados tales como Antivirus y Firewalls personales.

La tecnología de análisis de integridad podrá aplicar acciones correctivas cuando detecte que existe una faltante dentro del sistema.

La tecnología de análisis de integridad podrá aplicar acciones tales como descargar software, enviar a ejecutar aplicaciones, modificar llaves de registro, entre otros.

La tecnología de análisis de integridad deberá poder ejecutar scripts creados por el administrador en los equipos en donde se maneje una lógica simple de programación (Si la llave de registro es XXXX haga YYYYY).

Características de control de aplicaciones para protección de sistema Operativo:

La tecnología de protección de la solución al sistema operativo debe incluir mecanismos que eviten la ejecución de procesos maliciosos, estos procesos deberán poder ser definidos a través de políticas.

La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, lectura o modificación de archivos o directorios. Estos deberán poderse definir a través de políticas.

La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, modificación o eliminación de llaves de registro. Las llaves de registro a proteger deberán definirse por medio de políticas.

Características de bloqueo de dispositivos:

La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de los siguientes dispositivos: USB, bluetooth, PCMCIA, SCSI. Tarjetas inalámbricas, además deberá permitir la definición de nuevos dispositivos por medio del Class ID y Device ID.

La tecnología de bloqueo de dispositivos de la solución deberá permitir la creación de exclusiones para permitir el bloqueo de USB, pero no del teclado y el Mouse, por ejemplo.

La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de ejecución de programas desde dispositivos removibles.

La tecnología de bloqueo de dispositivos de la solución deberá permitir utilizar los dispositivos removibles como solo lectura.

Instalación de la Solución de acuerdo a los requerimientos de la Universidad Michoacana

Arquitectura de Ambiente Distribuido. De acuerdo a la política de tolerancia a fallas de la institución, la herramienta de administración estará en la capacidad de replicarse a nivel de: paquetes de instalación de clientes, logs, contenido de seguridad.

Listas de Servidores de Administración para Tolerancia a fallos. Se debe proveer la capacidad de generar un listado de Servidores con determinada prioridad, los cuales pueden atender requerimientos de actualización de políticas y contenido de seguridad de parte de los clientes de protección.

PARTIDA	CANTIDAD	DESCRIPCION DE LOS BIENES	BENEFICIARIO	LUGAR DE ENTREGA
12	1	<p>8.2.2.1.81 Analizador de Calidad de la Energia Eléctrica con sondas de corriente flexibles de 3,000 A, Amprobe DM-5, configuración rápida con guía paso a paso que permite hacer mediciones sin errores, monitoreo en tiempo real en PCs y dispositivos compatibles vía Bluetooth, medición simultanea de potencia, armónicos, forma de onda, calidad eléctrica (voltaje en 3 canales, corriente en 4 canales), análisis completo mediante el software incluido con generación de reportes y visualización de datos para identificar rápidamente problemas potenciales, parámetros de prueba: voltaje, corriente, potencia activa/reactiva/aparente, factor de potencia y frecuencia, todos en la misma pantalla, eventos de calidad eléctrica: transitorios, corriente de arranque, filker, interrupciones, picos, y caídas, memoria para auto registro de hasta 1000 parámetros en intervalos definidos por el usuario, sensor de corriente AC CT-53 con 3 pinzas flexibles con selección de rango de entrada (300A, 1000A y 3000A), Pinza flexible de corriente AC CT-500 de 1000A, 4 cables de prueba con clips de caimán (rojo/negro/azul/verde), cable de alimentación americano, tarjeta de memoria SD (2G), cable USB, 32 sujetadores de cable (8 colores), 6 pilas AA, software pa PC en CD y maleta de transporte.</p>	<p>MIGUEL ROQUE VÁZQUEZ HERNÁNDEZ</p>	<p>LABORATORIO DE ELÉCTRICA</p>

13	4	<p>8.2.2.1.62 Generador de funciones BK Precisión 4052, Generador de funciones DDS Arbitrario con ancho de banda de 5 MHz con una velocidad de muestreo de 125MSa/s, amplitud de registro de hasta 16 Kp, tiempo de subida \leq a 7nS tiene una amplitud de carga de 0 a 10V punto a punto (50Ω); display a color LCD, comunicación USB; este modelo cuenta con las funciones: AM, DSB-AM, ASK, FM, FSK, PM, PWM, entre otras.</p>	ISRAEL LUNA REYES	LABORATORIO DE ELECTRÓNICA INDUSTRIAL
15	1	<p>8.2.2.1.5 Prensa eléctrica digital para ensaye a compresión, alcance de medición 135000 kgf, bomba con válvula regulable de aplicación de carga; manómetro ADR touch con resolución desde 1 kgf, unidades de medición lbf, kN y kgf, interface USB, memoria interna de 2 GB configuración del tipo de muestra, indica la velocidad de aplicación y retención de carga máxima, determina la resistencia, dos modos de calibración, incluye equipo para módulo de elasticidad en especímenes de 10 x 20 cm; dos indicadores de cuadrante análogos.</p>	CINDY LARA GOMEZ	LABORATORIO DE MATERIALES: MORELIA, MICHOACÁN.