Anexo 1
CARACTERÍSTICAS TÉCNICAS MÍNIMAS DE LOS BIENES A ADQUIRIR

3.1 COMPONENTE SERVIDOR (INFRAESTRUCTURA TECNOLÓGICA PARA SOFTWARE RIS-PACS):

Este componente se encuentra conformado por los ítems:

ITEM	DESCRIPCIÓN	CANTIDAD
1	Solución HCI	1
2	Solución de Respaldo	1

3.1.1 ITEM 1: SOLUCIÓN HCI

CARACTERÍSTICAS	DESCRIPCIÓN
Características Generales	Debe ser de propósito específico, donde todos los componentes de hardware deben ser de la misma marca.
	Debe ser nuevo (de primer uso), no catalogado como descontinuado o "end of life" o "end of sale", deberá estar vigente tecnológicamente, pertenecer a la última versión o generación liberada por el fabricante y ser fabricado en el año de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, mediante documentación oficial de la subsidiaria del fabricante en Perú con referencia al presente proceso.
Tecnología	Debe estar basada en tecnología hiperconvergente (HCI) o tecnología hiperconvergente desagregado (dHCI), que entregue un almacenamiento **All-NVMe**, con características de eficiencia habilitadas y licenciadas, y además, pueda integrar la gestión de Cómputo y Almacenamiento en una consola unificada bajo la misma herramienta.
Componentes de la solución	Debe ser una solución hiperconvergente o hiperconvergente desagregado de fábrica (debe ser instalado y configurado de fábrica), el cual debe incluir todos los componentes necesarios para su puesta en operación y debe contar con los siguientes componentes: • Nodos de cómputo • Virtualización de Cómputo • Almacenamiento • Gestión unificada.
Escalabilidad	Debe tener la capacidad de crecimientos modulares en el mismo clúster horizontal y verticalmente, estos crecimientos deben incrementar las capacidades de cómputo, memoria, conectividad de red y almacenamiento en forma independiente o crecer de forma desagregada.
Características Técnicas	Producto certificado y catalogado por el fabricante como SISTEMA HIPERCONVERGENTE (HCI) o SISTEMA HIPERCONVERGENTE DESAGREGADO (DHCI).

Hospital de Emergencias Jose Casimiro Ulloa
Firmado digitalmente por ALLPAS GOMEZ Henry Lowell FAU 20138100015 soft
Motivo: Doy V° B°
Fecha: 06.02.2025 17:57:56 -05:00

Hospital de Emergencias Jose Casimiro Ulloa
Firmado digitalmente por OCHOA DELGADO Isabel Milagros FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:10:38 -05:00

Hospital de Emergencias Jose Casimiro Ulloa
Firmado digitalmente por SILVA BUITRON Giancarlos FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:05:02 -05:00

Hospital de Emergencias Jose Casimiro Ulloa
Firmado digitalmente por PACHAS SUAREZ Carlos Abraham FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:01:10 -05:00

	Las actualizaciones de software, firmware, parches/fixes deben ser certificadas y entregadas por el fabricante, considerando todos los componentes de red, cómputo, almacenamiento y virtualización. debe contar con una aplicación de gestión que unifique la descarga automática de parches/fixes, así como detalles de parches/fixes soportados y su procedimiento de aplicación. No podrán ser aplicadas actualizaciones y/o parches que no hayan sido pre-validados y liberados por el fabricante. Las actualizaciones del Sistema Operativo, del firmware y del hipervisor deben ser en caliente sin interrupción del servicio.
	Debe contar con un esquema de atención directa de llamadas y problemas que deberá ser provisto desde un centro de soporte unificado del fabricante, desde donde deberán asistirse todos los problemas asociados a los componentes de red, cómputo, almacenamiento y virtualización, durante el tiempo que dure la garantía en la modalidad 7 x 24 x 365 por 5 años. Se debe garantizar para la presentación de la propuesta, con documentación emitida por la subsidiaria del fabricante en Perú con referencia al presente proceso.
	Debe incluir todo el licenciamiento e instalación del software hipervisor que permita el cumplimiento de todo lo requerido. Se deberá detallar en la propuesta la cantidad y versión de todo el licenciamiento necesario para cumplir con el objeto de la contratación y sin costo adicional para la institución; este licenciamiento tendrá actualizaciones y/o suscripciones por el tiempo de 5 (cinco) años a partir de la suscripción del acta de entrega recepción final.
Replicación	La solución deberá contar con funcionalidades de replicación nativa sin requerir de software de terceros o de hardware adicional, así mismo deberá contar con mecanismos de optimización de la transferencia de datos para minimizar el uso de ancho de banda requerido para replicar.
Disponibilidad	La solución ofertada debe garantizar como mínimo 99.9999% de disponibilidad. Se debe acreditar para la presentación de la propuesta, con información pública y oficial del fabricante acompañado del link donde se substrajo dicha información.
Licenciamiento	Cada nodo de cómputo deberá contar con el licenciamiento del hypervisor ofertado con 5 años de soporte.
Protección de Datos	La solución ofertada deberá contar con funcionalidades de protección de datos que permitan la recuperación de una VM o de un conjunto de VMs en un punto en el tiempo, esta protección deberá utilizar técnicas de optimización de datos como la deduplicación de forma que se minimice el almacenamiento requerido para ello. Esta protección deberá

	poderse llevar a cabo tanto de forma local como remota hacia un centro de datos alterno.
Redundancia	Toda la infraestructura y sus componentes de red, cómputo, almacenamiento y virtualización deberán ser con esquema de alta redundancia. Se debe incluir en la propuesta el certificado u Hoja de datos respectivas.
Monitoreo Global y Visibilidad	• Contar con una consola de inventario de activos que permita una vista global de todos los activos de cómputo y almacenamiento asociados a la consola. • Contar con un panel de control operativo que permita una vista detallada y acceso a hipervínculos de componentes de la infraestructura. • Contar con estadísticas de recursos que permitan vistas detalladas que muestran estadísticas de componentes de infraestructura como CPU, memoria, capacidad de almacenamiento. • Contar con visualizaciones de rendimiento que entreguen gráficos y cronogramas codificados por colores que indican latencia, IOPS de lectura / escritura, rendimiento, uso de capacidad, saturación de rendimiento e impacto potencial del almacenamiento. • Contar con alertas de bienestar (detección basada en reglas) que entregue alertas de bienestar basadas en reglas o umbrales. • Contar con un panel de control ejecutivo que entregue una vista consolidada de todos los componentes del almacenamiento, incluida la eficiencia de la capacidad total, los casos de soporte cerrados automáticamente y manualmente, el estado de protección de datos desglosado por carga de trabajo y/o aplicación y recomendaciones de actualización de hardware. • Debe entregar recomendaciones preventivas para reducir las conjeturas sobre la administración de la infraestructura y la confiabilidad de la aplicación.
Analítica de rendimiento	• La plataforma deberá ser capaz de monitorear y analizar todos los componentes de la infraestructura, desde el almacenamiento hasta el Hypervisor y las máquinas virtuales. • Contar con analítica de máquinas virtuales y diagnóstico que permita una vista completa con estadísticas de todos los componentes de la herramienta centralizada de monitoreo de la

	plataforma virtual, incluidos: Centros de datos, clústeres, hosts virtuales ESXi, datastores, máquinas virtuales y vmdks. • Permite identificar las causas de problemas de desempeño, mapas de calor de todo el entorno virtual que muestre áreas problemáticas, rendimiento por vmdk, tendencias de capacidad del almacén de datos y hosts virtuales sobrecargados. • Contar con puntuación de impacto potencial a través del uso de puntuación que muestra potenciales problemas. Permita deducir qué eventos son preocupantes según la carga de trabajo. • Permite señalar visualmente dónde pueden estar las áreas de posibles problemas. • Incluir un análisis instantáneo de la causa raíz para ambientes virtuales: Identifica proactivamente posibles problemas del rendimiento en el almacenamiento, los servidores, las máquinas virtuales y la conectividad. • Permite entregar recomendaciones personalizadas para mejorar/optimizar el rendimiento de la plataforma virtual y el sistema de almacenamiento con instrucciones para aplicarlas. • Permite visualizar el rendimiento del almacenamiento disponible para futuras cargas de trabajo. • De ser necesario se debe incluir todo el licenciamiento necesario para poder entregar estas características.
Redundancia de energía y ventilación	La solución debe tener redundancia en sus fuentes de poder y sistemas de ventilación, estos deben soportar reemplazo en caliente.
Garantía y Soporte	Debe ser brindada directamente por el fabricante, acorde a los procedimientos y políticas establecidos por la subsidiaria del fabricante en Perú y entregado de forma unificada (hardware de los Nodos, Almacenamiento, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión), a través de un servicio de soporte integral y unificado que garantice ser entregado por la misma marca.
	Debe cubrir fallas o defectos de fabricación, que puedan manifestarse durante su uso normal y en las condiciones imperantes.
	Debe ser por el periodo de 05 años, 24x7 con 4 horas de tiempo de respuesta, el cual incluye reparación o de ser el

	caso sustitución del componente o total de componentes ofertados.
CAPACIDADES DE ALMACENAMIENTO	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Funcionalidades	El Hipervisor debe soportar e incluir como mínimo funcionalidades de alta disponibilidad, movimiento en caliente de máquinas virtuales, distribución automática de recursos.
Resiliencia	La plataforma ofertada deberá contemplar la cantidad de nodos necesarios para garantizar un alto nivel de resiliencia. Para ello se requiere que la solución ofertada entregue mínimamente un nivel de protección del tipo RF3, FTT2 y/o perdida mínima de 2 discos de forma simultánea en nodos diferentes dentro del mismo clúster sin pérdida de información, considerando una configuración N+1.
Almacenamiento	El fabricante de la solución hiperconvergente debe proveer todo el licenciamiento necesario para activar el almacenamiento y tener habilitadas las características de compresión y deduplicación e incluir el soporte integrado de virtualización de almacenamiento.
Recursos compartidos	El sistema de almacenamiento debe proveer recursos de bloques a sistemas fuera del Sistema Hiperconvergente a través de protocolos estándares como FC, iSCSI, etc.
Gestión	La administración de la virtualización de almacenamiento debe ser integrada a la administración de servidores virtuales.
Integración	El almacenamiento ofertado deberá soportar y estar certificado para vVOL y VASA.
Características necesarias	El sistema de almacenamiento debe manejar como políticas características mínimas como: • Compresión y deduplicación habilitados. • Desempeño • Nivel de protección • Calidad de Servicio
NODOS DE CÓMPUTO	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Cantidad de nodos	La solución hiperconvergente debe incluir 5 nodos como mínimo:
NODO TIPO 01	**CANTIDAD 03**
Factor de Forma	Formato Rackeable de hasta 02 RU (unidades de rack) por nodo, para ser alojado en rack de 19".
Escalabilidad	El Sistema HIPERCONVERGENTE debe tener una escalabilidad mínima de 32 nodos de cómputo.
Redundancia de energía y ventilación	La solución debe contar con todas sus fuentes de poder y ventiladores para una alta disponibilidad

Cantidad de Cores	Mínimo dos procesadores de tecnología x86 por nodo, cada procesador debe tener al menos 16 Cores y 2.9 GHz de frecuencia base
Memoria RAM	Cada nodo debe tener al menos 1 TB usables por Nodo de cómputo (módulos de 64Gb como mínimo). Los recursos de Overhead requeridos para la hiperconvergencia (RAM y CPU) deberán ser contemplados por el oferente como recursos adicionales a lo solicitado por la Institución y sustentando con la herramienta oficial de sizing del fabricante.
	El tipo de memoria incluida en cada nodo debe ser del Tipo DDR4 3200MHz. Los módulos DIMM deben integrar la tecnología de memoria tolerante a fallas que permite que el sistema detecte y corrija errores de memoria antes de que los errores puedan afectar negativamente al sistema, lo que mejora la resistencia del sistema a los problemas de memoria.
Conectividad LAN por nodo	Mínimo 4 puertos de red 25GbE por cada nodo de cómputo y un puerto de al menos 1Gbps para administración
Controlador RAID	• Tipo SAS. • Debe incluir RAID 0 y 1 con 2GB de memoria cache. • Debe incluir encriptación de discos bajo el estándar FIPS140-2, de no soportar encriptación los discos deberán ser de tecnología autoencriptable (SED) como mínimo.
Discos de Arranque	Cada nodo debe contar con dos (02) discos de booteo de tecnología SSD y cada uno de los discos con un mínimo de capacidad de 480GB SSD M.2
Memoria cache	Para soluciones hiperconvergentes basadas en nodos, la solución debe contener almacenamiento en disco para memoria cache de 10 TB.
Capacidad de Almacenamiento requerida	La capacidad usable por clúster mínima debe ser 90 TB NVMe, la solución deberá tener habilitada la funcionalidad de compresión y deduplicación garantizando así una mayor capacidad efectiva. Esta deberá conectarse por interfaz de red y deberá correr a 10/25GB ISCSI.
Software requerido	Deberá contar con las siguientes características integradas: • Software de administración, de monitoreo, de Acceso remoto, de reportería.
Seguridad	Los servidores deberán contar con elementos de protección contra ataques de ransomware embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso, incluso antes del arranque del hipervisor/sistema operativo, estos mecanismos deberán contar con elementos de recuperación de firmware a un

	estado saludable en caso de presentarse un escenario de intrusión avanzado.
NODO TIPO 02	**CANTIDAD 02**
Factor de Forma	Formato Rackeable de hasta 02 RU (unidades de rack) por nodo, para ser alojado en rack de 19".
Escalabilidad	El Sistema HIPERCONVERGENTE debe tener una escalabilidad mínima de 32 nodos de cómputo.
Redundancia de energía y ventilación	La solución debe contar con todas sus fuentes de poder y ventiladores para una alta disponibilidad
Cantidad de Cores	Mínimo dos procesadores de tecnología x86 por nodo, cada procesador debe tener al menos 16 Cores y 2.9 GHz de frecuencia base
Memoria RAM	Cada nodo debe tener al menos 1 TB usables por Nodo de cómputo (módulos de 64Gb como mínimo). Los recursos de Overhead requeridos para la hiperconvergencia (RAM y CPU) deberán ser contemplados por el oferente como recursos adicionales a lo solicitado por la Institución y sustentando con la herramienta oficial de sizing del fabricante.
	El tipo de memoria incluida en cada nodo debe ser del Tipo DDR4 3200MHz. Los módulos DIMM deben integrar la tecnología de memoria tolerante a fallas que permite que el sistema detecte y corrija errores de memoria antes de que los errores puedan afectar negativamente al sistema, lo que mejora la resistencia del sistema a los problemas de memoria.
Video	Cada nodo debe tener al menos una tarjeta gráfica de 16GB PCIe
Conectividad LAN por nodo	Mínimo 4 puertos de red 25GbE por cada nodo de cómputo y un puerto de al menos 1Gbps para administración
Controlador RAID	• Tipo SAS. • Debe incluir RAID 0 y 1 con 2GB de memoria cache. • Debe incluir encriptación de discos bajo el estándar FIPS140-2, de no soportar encriptación los discos deberán ser de tecnología autoencriptable (SED) como mínimo.
Discos de Arranque	Cada nodo debe contar con dos (02) discos de booteo de tecnología SSD y cada uno de los discos con un mínimo de capacidad de 480GB SSD M.2.
Memoria cache	Para soluciones hiperconvergentes basadas en nodos, la solución debe contener almacenamiento en disco para memoria cache de 10 TB.
Capacidad de Almacenamiento requerida	La capacidad usable por clúster mínima debe ser 90 TB NVMe, la solución deberá tener habilitada la funcionalidad de compresión y deduplicación garantizando así una mayor

	capacidad efectiva. Esta deberá conectarse por interfaz de red y deberá correr a 10/25GB ISCSI.
Software requerido	Deberá contar con las siguientes características integradas: Software de administración, de monitoreo, de Acceso remoto, de reportería.
Seguridad	Los servidores deberán contar con elementos de protección contra ataques de ransomware embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso, incluso antes del arranque del hipervisor/sistema operativo, estos mecanismos deberán contar con elementos de recuperación de firmware a un estado saludable en caso de presentarse un escenario de intrusión avanzado.
PLATAFORMA DE VIRTUALIZACION	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Características Generales	Licenciamiento de software de virtualización de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, el cual: • No debe estar asociado a servidor físico. • Debe permitir la instalación en otro hardware (de la misma marca) de ser necesario.
Características Técnicas	Las funciones de administración de cómputo y almacenamiento virtualizado deben ser integradas en una sola consola. Debe proveerse una consola integrada tipo GUI para realizar funciones de gestión. Al menos debe contar con todas las siguientes características: • Aprovisionamiento de nodos nuevos. • Actualización de parches de software del sistema, hipervisor y firmware en caliente. • Visualizar la utilización de los recursos. • Visualizar el estado de salud del sistema
Software de virtualización	La solución de hiperconvergencia debe incluir el hipervisor con suscripción, con actualizaciones y soporte por mínimo 5 años.
Licenciamiento Hiperconvergente	El SISTEMA HIPERCONVERGENTE debe incluir la suscripción para la plataforma de virtualización de acuerdo con el equipamiento propuesto. Se deberá detallar las especificaciones las suscripciones propuestas.
Versión de SW	Se debe instalar en los respectivos nodos, la última versión estable, liberada y soportada por el fabricante del SISTEMA HIPERCONVERGENTE a la fecha de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, con documentación emitida por la subsidiaria del fabricante en Perú con referencia al presente proceso.

Licenciamiento precargado	En el Sistema HIPERCONVERGENTE se debe incluir y venir pre-cargado el Hipervisor y todo el resto de software necesario, de modo de minimizar los tiempos de puesta en marcha.
Funcionalidades	El Hipervisor debe soportar e incluir como mínimo funcionalidades de alta disponibilidad, replicación, movimiento en caliente de máquinas virtuales, distribución automática de recursos entre nodos.
Administración	Se debe incluir una consola de administración centralizada que permita administrar todos los hosts que se puedan crear en la infraestructura.
LOGS y Registro	El Hipervisor debe proveer una funcionalidad de registro o LOG integrada de modo de proveer una visión de los eventos de hardware y software.
Alta Disponibilidad	La solución deberá incluir estadísticas completas sobre las máquinas virtuales, como consumo de vCPU, RAM y Disco, así como los IOPs de lectura/escritura y latencia.
SERVICIOS DE ALMACENAMIENTO	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Características Técnicas	El fabricante del Sistema HIPERCONVERGENTE (HCI) o SISTEMA HIPERCONVERGENTE DESAGREGADO (DHCI), debe proveer el soporte integrado acorde al SLA de estas aplicaciones de servicios de almacenamiento, mientras dure la garantía técnica de la solución. El Postor para la admisión de su propuesta, deberá incluir un documento emitido por la subsidiaria del fabricante en Perú, para la verificación del cumplimiento de este requerimiento, en su nivel más alto de soporte para equipamiento de misión crítica.
	El Sistema debe soportar la funcionalidad de replicación de máquinas virtuales a un sistema externo.
	La replicación deberá permitir replicación con RPO = 0 (es decir replicación sincrónica).
	Todas las funcionalidades de la plataforma deberán estar habilitadas desde el primer día (Compresión, Duplicación, Encriptación, Replicación, etc) sin restricciones en la capacidad de almacenamiento, se deberá incluir todas las licencias necesarias si son requeridas por la solución ofertada.
	En caso de una solución HCI basada en nodos se deberán poner al menos dos discos de cache por nodo para garantizar el desempeño de la solución.
	Deberá entregar como mínimo 97,000 IOPS con una distribución de 50% lectura / 50% escritura.
ADMINISTRACIÓN DEL SISTEMA HIPERCONVERGENTE	
CARACTERÍSTICAS	**DESCRIPCIÓN**

Características Técnicas	Las funciones de administración de cómputo y almacenamiento virtualizado deben ser integradas en una sola consola. Debe proveerse una consola integrada tipo GUI para realizar funciones de gestión. Al menos debe contar con todas las siguientes características: • Aprovisionamiento de nodos nuevos. • Actualización de parches de software del sistema, hipervisor y firmware en caliente. • Visualizar la utilización de los recursos. • Visualizar el estado de salud del sistema.
	Debe proveer la funcionalidad de alarmas preventivas y automáticas en caso de falla de componentes del sistema a través de correo electrónico.
	El sistema debe contar con un software de gestión que mínimo cumpla con las siguientes funcionalidades: • Descubrir y mantener automáticamente el inventario de toda la infraestructura del sistema. • Chequeo de las versiones de software instaladas en el sistema versus las versiones de software certificadas por el fabricante. • Log HIPERCONVERGENTE o HIPERCONVERGENTE DESAGREGADO del sistema. • Monitoreo del estado de salud de la infraestructura.
	La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia o hiperconvergencia desagregada, manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información.
	El servicio de administración debe ser gestionado desde una consola permitiendo al menos lo siguiente: • Gestionar todos los componentes de la solución hiperconvergente o hiperconvergente desagregada. • Soporte para monitoreo de los hipervisores centralizadamente. • Asignar roles de usuario basado en perfiles por lo que la solución soportará la integración con Directorio Activo o con sistemas LDAP para la autenticación en el uso de la herramienta. • Debe tener interfaz gráfica de administración basada en un entorno WEB de uso intuitivo amigable al usuario.
	Debe permitir determinar en tiempo real el consumo de los

	recursos de CPU, Memoria RAM y almacenamiento por nodo, por máquina virtual, por clúster y en forma global.
	La interface gráfica debe entregar mínimo estadísticas completas sobre las máquinas virtuales como consumos de vCPU, Memoria RAM y discos, así como: IOPS de lectura, IOPS de escritura y métricas de red.
	La solución debe permitir el análisis de ancho de banda utilizado por una máquina virtual, un host físico, o un clúster.
	La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, cómputo e hipervisor) directamente desde la consola y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni ocurrencia de indisponibilidad del servicio.

INCLUYE LICENCIA DE SOFTWARE VDI CON LAS SIGUIENTES CARACTERISTICAS:

MODULO DE VIRTUALIZACIÓN	
CARACTERÍSTICA	**DESCRIPCIÓN**
Características generales	Licenciamiento de software de virtualización de escritorio de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 44 usuarios nombrados.
	Se debe considerar: o Licenciamiento de software de virtualización de escritorio. o Licenciamiento de sistema operativo Windows para escritorios virtuales.
	Licenciamiento, por el periodo de 05 años, el cual debe incluir derecho a actualizaciones y soporte 24x7, provisto directamente por el fabricante.
	Licenciamiento bajo modelo de suscripción, donde el enlace de comunicación a la Consola de Administración, VDIs y/o Aplicaciones sea ON-PREMISE.
	Se debe proporcionar el licenciamiento de todo el software necesario, para el funcionamiento del módulo de virtualización solicitado.
Administración de la solución	Debe permitir configurar, administrar y gestionar grupos de escritorios y aplicaciones virtuales a entregar, uso de licencias de escritorio, aprovisionamiento de imágenes de escritorio virtual, autenticación y control de autorizaciones.
	Debe contar con una herramienta o funcionalidad nativa de mesa de ayuda, en la que sea posible que un técnico intervenga en la sesión virtualizada.

	Debe permitir la interacción entre el administrador y el usuario mediante el envío de mensajes directamente desde la consola de monitoreo y soporte.
	Debe permitir la visualización de la imagen del escritorio virtual en varios monitores.
	Debe soportar políticas de impresión de tal manera que pueda configurarse, sin necesidad de cambios en los scripts de inicio de sesión, mediante la aplicación de GPO's y de forma nativa de la solución.
	Debe presentar un tablero con un resumen de la información de alerta para ver y remediar incidentes.
	Debe contar con una herramienta para monitorear el uso, salud y desempeño de la infraestructura, escritorios y protocolos.
	La herramienta de monitoreo debe tener registros para auditar el acceso a las máquinas virtuales.
Gestión de recursos virtualizados	Debe ser capaz de provisionar y controlar el acceso a los recursos virtualizados (aplicaciones y escritorios) ya sea en el modelo de sesión única o multisesión cuando se encuentre disponible.
	Debe tener recursos para aprovisionar y desaprovisionar máquinas virtuales bajo demanda, independientemente de donde se asigne este recurso.
	Debe implementar el aprovisionamiento y administración de recursos virtualizados en máquinas virtuales con los sistemas operativos Microsoft Windows 11 o superior, RHEL 8 o superiores y Windows Server 2022 o superiores.
	Debe contar con una herramienta integrada a la solución que permita el aprovisionamiento de máquinas virtuales desde una sola imagen central, de manera que los administradores tengan autonomía para entregar los recursos con las actualizaciones más recientes, cada vez que se realice el inicio de sesión.
	El aprovisionamiento y desaprovisionamiento de recursos (máquinas virtuales) debe ser opcional según demanda, y compatible con cualquier Hipervisor.
	Debe permitir la creación de varias máquinas virtuales automáticamente, basadas en la misma imagen del sistema operativo.
	Debe permitir la configuración de un grupo de escritorios virtuales en standby (o aprovisionado) que pueda atender la demanda de conexión de los usuarios de forma paulatina, evitando el desperdicio de recursos físicos con escritorios virtuales encendidos y sin uso, estos escritorios en modo standby deben ser activados en cada grupo de escritorios virtuales a través de la consola de administración.

	Debe permitir la creación de varios escritorios virtuales automáticamente, basados en una imagen de sistema operativo preconfigurada, acelerando la entrega de escritorios virtuales a usuarios no persistentes.
	Debe poder crear grupos persistentes de escritorios virtuales, es decir, grupos de escritorios virtuales que se pueden aprovisionar para el usuario y que, después del primer aprovisionamiento, solo puede acceder el mismo usuario.
	Debe ofrecer una herramienta de virtualización de aplicaciones que permita a los administradores de escritorio transformar aplicaciones compatibles con Microsoft Windows en aplicaciones portátiles que puedan ejecutarse sin necesidad de un Escritorio completo.
	Debe~~r~~ permitir la creación y uso compartido o dedicado de escritorios virtuales sobre plataformas Windows y distribuciones Linux, sin limitar el número de Escritorios de cada tipo hasta el total de licencias adquiridas en el presente procedimiento de selección.
Gestión de perfiles	La funcionalidad de gestión inteligente de perfiles debe ser una parte integrada de la solución, sin costo adicional.
	Debe proporcionar la funcionalidad de perfil móvil, es decir, conservar las personalizaciones del perfil de usuario y almacenarlas en un servicio de gestión de perfiles dinámicos, aplicando las características conservadas por el usuario a los recursos virtualizados (aplicaciones o escritorios) siempre que los usuarios inicien sesión.
	Debe permitir que el administrador use perfiles de solo lectura, que se descartan al cerrar la sesión, sin depender de los servidores de archivos.
	Debe permitir que el dispositivo redirija las carpetas a los servidores de archivos especificados. Se deben redirigir las carpetas de archivos de usuario predeterminadas, como las que se enumeran a continuación: Escritorio, Documentos, Videos, Imágenes, Música, Descargas, Favoritos, Contactos, Enlaces, Búsquedas, Menú Inicio y AppData.
	Debe permitir que la sincronización de los datos del perfil de usuario sea parcial, es decir, dando la posibilidad al administrador de seleccionar lo que debe o no sincronizar en el perfil de usuario, pudiendo realizar esta configuración de forma global o específica por usuario.
	Debe poseer una solución de transmisión de perfiles para que se pueda entregar de manera escalonada siguiendo la demanda del usuario, sin que el usuario tenga que esperar a que su perfil completo comience a usarlo.

	Debe permitir la sincronización de perfiles mientras el usuario está conectado, reduciendo así la carga excesiva de datos durante el cierre de sesión, realizando solo el delta al final del uso.
Experiencia del usuario	Debe proporcionar al usuario acceso a los recursos virtualizados desde un único portal, este portal de acceso debe estar disponible para acceso externo con alta disponibilidad en todos los Centros de Datos, sin embargo, la solución debe permitir que la sesión del usuario con el recurso virtualizado se establezca con el Centro de Datos más cercano al backend del servidor accedido por el recurso virtualizado.
	Debe proporcionar una aplicación cliente que permita al usuario a través de un dispositivo físico acceder a un escritorio virtual o aplicación publicada, compatible con los siguientes sistemas operativos: Windows, MacOS, Linux, Android, iOS y Chromebook.
	Debe permitir que los usuarios marquen sus aplicaciones y escritorios favoritos, que se agregarán a una página separada en su perfil.
	Debe contar con un cliente soportado para instalación y acceso a la plataforma para los siguientes Sistemas Operativos: Windows, Linux, MacOS, Android e IOS.
	Debe soportar el uso de estaciones tipo thin client que utilicen sistemas operativos basados en Linux y/o Microsoft Windows Embedded.
	Debe permitir; independientemente del método de acceso (cliente instalado o navegador web), la redirección multimedia, permitiendo así reproducir las aplicaciones de sonido en el sistema de sonido del dispositivo local.
	Debe permitir al usuario utilizar un navegador web para acceder, a través del protocolo HTTPS, a un escritorio virtual o aplicación publicada, si el dispositivo físico utilizado no permite la instalación de la aplicación cliente de la solución ofrecida.
	Debe permitir a los usuarios controlar los recursos de sonido, el tamaño de la ventana y reiniciar su escritorio virtual sin necesidad de la intervención del administrador, excepto para reiniciar los escritorios virtuales que funcionan con multisesión.
	Debe permitir al usuario continuar con su trabajo, exactamente donde lo dejó, en caso de que necesite cambiar de estación de trabajo o abrir una sesión en otro tipo de equipo. Esta funcionalidad debe cerrar la sesión de usuario abierta en el dispositivo inicial y abrirla en el nuevo

	dispositivo, lo que permitirá que el escritorio "siga" al usuario.
	Debe admitir de forma nativa y realizar la optimización del tráfico con respecto a las herramientas de colaboración más utilizadas, como Microsoft Teams, Zoom y Cisco Webex.
	Debe permitir el uso de tokens criptográficos y tarjetas inteligentes para firmar documentos en escritorios virtuales.
	La herramienta debe ser capaz de facilitar la interacción del usuario al acceder a aplicaciones y/o escritorios a través de dispositivos táctiles, optimizando las funciones emergentes del teclado, el desplazamiento de la pantalla y el zoom automático
Seguridad	Debe ofrecer un portal de autoservicio capaz de integrarse con la solución de virtualización de escritorio y otras aplicaciones Web, con el fin de unificar la experiencia del usuario y aumentar la seguridad en el acceso a los datos, aplicando configuraciones de autenticación de acceso condicional y de doble factor.
	Debe permitir el acceso a escritorios y aplicaciones virtualizadas a través de un portal disponible vía Web, con autenticación segura y acceso vía SSL o TLS.
	Debe controlar las acciones de “copiar y pegar” entre la máquina del usuario y el contenido accedido.
	Debe tener recursos para controlar la captura de pantalla de los recursos virtualizados (anticaptura de pantalla).
	Debe disponer de recursos para evitar la captura/ copia de información tecleada durante el acceso a los recursos virtualizados (Anti-keylogger o similar).
	Debe restringir o permitir que el contenido disponible se imprima en impresoras conectadas al dispositivo del usuario.
	Debe permitir o bloquear la conexión de los periféricos de los usuarios con los escritorios y aplicaciones virtualizadas, tales como: discos locales, unidades de red, CD-ROM, DVD-ROM y dispositivos extraíbles (pendrive, HD externo, etc.).
	Debe poner a disposición, en la interfaz de acceso, únicamente los escritorios virtuales o aplicaciones publicadas a los que el usuario tenga acceso, observando los permisos y privilegios definidos luego del proceso de autenticación y análisis del dispositivo.
	Debe contar con recursos para controlar los cambios realizados en el entorno de virtualización de aplicaciones y escritorios, de manera que, cuando sea necesario, los administradores tengan acceso a logs con los cambios

	realizados en la configuración o permisos del entorno, con fecha y autor de los cambios
MODULO DE SEGURIDAD DE ACCESO	
DESCRIPCIÓN	**CARACTERÍSTICAS TÉCNICAS**
Características generales	Certificado Digital SSL por el período de 5 años.
Seguridad de segundo factor de autenticación	Debe soportar acceso a los usuarios a través de un portal, que deberá contener asociado de un certificado digital TLS/SSL de una entidad de certificados públicos de confianza, como mínimo contener algoritmo RSA Public Key SHA-2, Compatibilidad con el cifrado de claves públicas de 2.048 bits.
Seguridad de segundo factor de autenticación	Debe implementar una autenticación multifactor, que permita que los usuarios puedan usar una aplicación de autenticación instalada en su dispositivo para generar un código de acceso como segundo factor de identificación en el proceso de inicio o ingreso a la solución.
MODULO DE SEGURIDAD DE VIRTUALIZACIÓN	
DESCRIPCIÓN	**CARACTERÍSTICAS TÉCNICAS**
Características generales	Licenciamiento de software antimalware de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 100 escritorios virtuales.
	Licenciamiento por el periodo de 05 años, el cual debe incluir derecho a actualizaciones y soporte 24x7.
	El licenciamiento de software antimalware debe ser gestionado a través de una consola implementada en los servidores de la Entidad.
	El software debe incluir un sistema de análisis de vulnerabilidades derivadas de plataformas Windows y programas de terceros que permita la descarga centralizada de parches, la aplicabilidad, la distribución y la instalación remota de estos. Este sistema debe estar integrado al software antimalware por lo que no deberá requerir la instalación de ningún componente adicional para su normal desempeño.
	El software antimalware debe estar en idioma español.
	Deberá contar con un sistema de distribución y despliegue centralizado permitiendo en determinados casos generar instaladores independientes y personalizados.
	La consola de administración debe poder instalarse en sistemas operativos tales como Windows Server 2022 o posterior.
	La consola de administración deberá poder lanzar tareas de despliegue de clientes de forma remota.

Gestión y gobierno centralizado	La consola de administración deberá poder mostrar un resumen de la instalación indicando el estado y sugiriendo una acción de refuerzo si fuese necesario.
	La consola deberá ser 100% web permitiendo implementar una nube privada a través de un componente web seguro (https), a fin de poder gestionar los escritorios virtuales de la red corporativa de forma transparente.
	La consola de administración deberá poder registrar eventos creando logs por cada uno de los eventos que realice dependiendo del ítem (exploración, actualización, bloqueos, etc.)
	La consola de administración deberá permitir implementar exclusiones en la exploración, con capacidad para excluir de la exploración archivos, directorios y/o procesos, etc.; de forma centralizada.
	La consola de administración deberá permitir la programación de tareas, capacidad para programar tareas de exploración, actualización, etc.
	La consola de administración deberá permitir la configuración de repositorios para actualización, capacidad para agregar/eliminar repositorios hacia donde se descarga la actualización de las definiciones de virus.
	La consola de administración deberá permitir la instalación remota, pudiendo lanzar tareas de instalación en clientes de forma remota desde un servidor de administración antivirus.
	La consola de administración deberá mostrar un inventario general de todos los escritorios virtuales, logrando especificar los recursos de cómputo y almacenamiento que tienen instalado todos y cada uno de los escritorios virtuales protegidos.
	La consola de administración deberá poder programar análisis de malware en todos los escritorios virtuales sin que esto implique una saturación del procesador o memoria para realizar esta actividad, para esto se deberá poder especificar que el escaneo se realice utilizando los tiempos muertos del usuario, el objetivo es evitar saturar los recursos cuando el usuario los necesite.
	La consola de administración deberá contar con una cuarentena local capaz de aislar posibles amenazas de malware no firmadas, pudiendo liberar y limpiar programas y/o aplicaciones según convenga el administrador.
	La consola de administración deberá poder reportar y enviar directamente al fabricante, software y/o amenazas no firmadas para su evaluación.

	La consola de administración deberá poder integrarse con el directorio activo a fin de llevar una sola gestión (grupos organizativos)
	La consola de administración deberá tener la capacidad de definir políticas de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para configuraciones de objetos específicos (Módulos de protección).
	La consola de administración deberá estar desarrollada sobre una arquitectura multitenant a fin de poder implementar de forma transparente nuevos escenarios de protección en diferentes redes a nivel nacional en el tiempo, integrando la gestión de diferentes consolas con sus propios recursos y condiciones en una sola.
	Este sistema deberá tener la capacidad de generar reportes locales en cada escritorio virtual, referentes a todas las transacciones realizadas por cada producto.
	Deberá permitir la actualización independiente de productos para aquellos equipos que no puedan sincronizar con la consola.
Tecnología antimalware	Deberá proteger sistemas operativos como Windows Server 2022 o superior y Windows 11 o superior.
	Deberá incluir un sistema de análisis basado en algoritmos heurísticos capaces de detectar malware por similitud.
	Deberá incluir un sistema que optimice la detección y eliminación de malware empaquetado usado para saturar el performance de los residentes antivirus lanzando miles de variables a partir de un malware ya conocido.
	Deberá incluir tecnología basada en el análisis del comportamiento de amenazas logrando detenerlas incluso sin estar firmadas.
	Deberá contar un módulo de protección especialmente diseñado para hacerle frente a todo tipo de amenazas de tipo RANSOMWARE cual deberá permitir poner en cuarentena la amenaza y si fuese necesario incluir una lista blanca de aplicaciones específicamente para este módulo.
	Deberá poder reconocer y bloquear amenazas de día cero basadas en vulnerabilidades del sistema operativo y programas instalados.
	Deberá incluir tecnologías de Machine Learning que le permitan automatizar el aprendizaje de nuevas amenazas de malware a través de sus diferentes sensores o tecnologías propuestas.
	Deberá contar con tecnologías de inteligencia artificial y aprendizaje automático capaz de reconocer y actuar sobre ataques de tipo malware ofuscado.

Atributos de prevención	Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de aplicaciones, el mismo que deberá poder definir aplicaciones en lista negra para evitar que estas se ejecuten en los escritorios virtuales.
	El módulo de control de aplicaciones deberá poder implementar sus políticas de aplicaciones en lista negras reconociendo el hash, versiones y fabricantes específicos de las aplicaciones a bloquear.
	El módulo de control de aplicaciones deberá tener un modo que permita la implementación de políticas de seguridad para el control de aplicaciones el mismo que deberá poder definir aplicaciones en lista blanca que permitan que solo estas puedan ejecutarse en determinados escritorios virtuales.
	El módulo de control de aplicaciones deberá poder aplicar políticas de seguridad a directorios y archivos específicos.
	El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su escritorio virtual, a fin de mejorar los tiempos de respuesta con el usuario.
	Deberá incluir una protección contra dispositivos USB físicos manipulados.
	Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos extraíbles, el mismo que deberá poder ser desplegado, habilitado o deshabilitado desde la consola de administración.
	El módulo de control de dispositivos deberá tener la capacidad de asignar privilegios de solo lectura a cualquier USB de almacenamiento externo que se conecte al escritorio virtual a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio.
	El módulo de control de dispositivos deberá permitir que el usuario pueda solicitar permiso de acceso a su dispositivo desde su escritorio virtual a fin de mejorar los tiempos de respuesta con el usuario.
	El módulo de control de dispositivos deberá permitir la creación de listas blancas especificas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento.
	Deberá tener un módulo que permita la implementación de políticas de seguridad para la navegación web el mismo que no debe necesitar instalar ningún tipo de plugin o componente adicional para escanear y filtrar contenido en los navegadores (Browsers soportados, Internet Explorer, Microsoft Edge, Firefox y Chrome).

	Deberá incluir un módulo que proteja las transacciones bancarias sin necesidad de implementar plugins ni componentes adicionales.
	Deberá incluir un módulo de monitoreo de redes que permita monitorear la red permitiendo la creación y análisis de métricas de evaluación para discos duros, servicios críticos, CPUs, impresoras, enrutadores, switches, servidores web, servidores de correo y servidores de base de datos a fin de establecer semáforos que faciliten la lectura de informes y alertas de anomalías presentadas en la red, a fin de detectar oportunamente tendencias de rendimiento.
	Deberá permitir implementar tareas de escaneo de malware en modo de reposo para de esta forma evitar saturar los recursos de los escritorios virtuales.
	El escaneo en modo de reposo permitirá definir carpetas y/o directorios específicos para su análisis.
	Deberá contar con módulo de protección que permita auditar la seguridad a nivel físico de cualquier dispositivo USB que se conecte al escritorio virtual asegurándose de que de este no esté corrupto con algún tipo de keylogger físico, el sistema deberá solicitar un código de seguridad cada que se conecte un nuevo dispositivo.
Atributos de mitigación	Deberá mitigar el daño provocado por contagios; cierra los puertos, monitorea aplicaciones y motores de correo electrónico, analice archivos y carpetas, que efectúe seguimientos y bloquee las comunicaciones que generen una infección.
	Deberá incluir protección que amenace específicamente las vulnerabilidades del sistema operativo, deberá incluir protección anti-exploit capaz de proteger de esas amenazas que aprovechan las brechas de seguridad en los programas instalados, desde editores de texto hasta plugins de los navegadores.
	Deberá contar con un módulo de gestión de parches centralizado capaz de reconocer vulnerabilidades que derivan de la ausencia de parches en el sistema operativo y programas instalados en los escritorios virtuales.
	El módulo de gestión de parches deberá ser capaz de clasificar los parches que necesitan aplicarse en los escritorios virtuales a fin de cerrar los huecos de seguridad encontrados, así como lanzar pruebas de aplicabilidad de los mismos a fin de asegurarse de que estos no ocasionen problemas de compatibilidad.

	El módulo de gestión de parches deberá ser capaz de realizar tareas de rollback (desinstalación remota de parches desde consola) en caso de requerirse.
	Deberá contar con un cortafuego administrable capaz de monitorear todo el tráfico entrante y saliente en todos y cada uno de los escritorios virtuales.
	El cortafuego deberá poder ser implementado en modo de piloto automático reconociendo todo el tráfico para luego implementar reglas específicas.
	El cortafuego deberá poder notificar cuando una aplicación sea bloqueada.
	El cortafuego deberá tener un asistente de configuración que permita implementar reglas de restricción y permiso a determinadas aplicaciones y puertos.
	Si el administrador así lo prefiere se podrá habilitar opción de desactivar cortafuego desde el cliente.
Atributos de detección	Deberá incluir tecnología innovadora para escritorio virtual que detenga y elimine proactivamente el software malicioso, extienda la cobertura contra nuevos riesgos de seguridad y reduzca el costo de respuesta frente a epidemias.
	Deberá permitir defender los sistemas contra virus, gusanos, troyanos, phishing, adware y spyware.
	Deberá bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria.
	Deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexión con servidores maliciosos de comando y detectar patrones típicos de equipos que forman parte de una Botnet.
	Deberá contar con protección contra ransomware que supervise el comportamiento de las aplicaciones y los procesos que intentan modificar los datos.
	Deberá bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica.
	Deberá proteger contra exploits dirigidos a aplicaciones y servicios Microsoft, especialmente a servicios del sistema operativo Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft Outlook.
	Deberá incluir un antivirus residente capaz de analizar diferentes protocolos de comunicación como HTTP, HTTPS, SMPT, POP, IMAP y otros.
	El residente antivirus deberá poder tomar diversas acciones en caso de una infección, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.

	El residente antivirus deberá poder tomar diversas acciones en caso de analizar archivos comprimidos, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.
	El residente de antivirus deberá poder configurarse en acceso a lectura, escritura y al ejecutar para que se esta manera se tenga mejor visibilidad de todos los archivos que se escriban en disco.
	El residente de antivirus deberá poder comprobar la existencia de virus informáticos en correos recibidos / enviados en el cliente de correo. Adicionalmente se podrá realizar la comprobación solo en los correos no leídos.
	El residente de antivirus deberá poder adjuntar un informe de ante un correo electrónico infectado.
	El residente deberá detectar y neutralizar amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes.
	Deberá contar con un módulo de copias de seguridad de información sensible que permita programar y ejecutar copias de seguridad de los archivos y carpetas más críticas en los clientes de forma diferencial y automática.
	El módulo de copias de seguridad debe escanear la data respaldada garantizando de esta manera de que se resguarden copias sin virus.
	El módulo de copias de seguridad debe permitir definir el destino de la información a respaldar, así como programar la tarea para determinado día con determinada frecuencia.
	El módulo de copias de seguridad debe permitir programar tareas de copias completas y parciales.
	El módulo de copias de seguridad debe permitir considerar exclusiones basado en extensiones, esto a fin de evitar respaldar música, videos y/o archivos de ocio del usuario.

3.1.2 ITEM 2: SOLUCIÓN DE RESPALDO

SERVIDOR DE BACKUP A DISCO	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Cantidad	Uno (01) unidad
Características Generales	Debe ser de propósito específico, donde todos sus componentes o partes deben ser de la misma marca; y, además, no se requiera de la instalación de software y/o hardware adicional que no forme parte del bien ofertado.
	Debe ser nuevo (de primer uso), no catalogado como

	descontinuado o “end of life” o “end of sale”, deberá estar vigente tecnológicamente, pertenecer a la última versión o generación liberada por el fabricante y ser fabricado en el año de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, mediante documentación oficial de la subsidiaria del fabricante en Perú con referencia al presente proceso.
Tamaño	Tipo rack de 2U
Procesadores	Dos (02) procesador de tecnología x86, debe tener al menos 8 Cores y 2.8 GHz de frecuencia base con fecha de lanzamiento igual o posterior a Q2 2021.
Chipset	Intel C621 Chipset
Memoria	64 GB (2 x 32GB) 16 DIMM por procesador, total 32 DIMMs, memoria DDR4 o superior. Capacidad de crecimiento a 3TB
Controlador RAID	Tipo SAS. Debe soportar RAID 0, 1, 5, 6, 10, 50, 60 con 4GB de memoria.
Almacenamiento	02 discos de booteo de tecnología SSD y cada uno de los discos con un mínimo de capacidad de 480GB SSD M.2 10 discos de 10TB SAS 12G de 7.2K en Raid 6 como mínimo Capacidad de crecimiento a 30 discos internos SFF Soporte de discos SAS Hot Plug de 6Gb y/o 12Gb en formatos de 2.5" y 3.5"
Interfaces	1 Display Port o VGA frontal 1 microSD 3 USB 3.0 (por lo menos 1 frontal y 2 posteriores, todos integrados)
Conectividad	2 puertos de red 25GbE y un puerto de al menos 1Gbps para administración 2 puertos FC de 16 Gb para la conexión con librería de respaldo en cinta
Slots de expansión	Capacidad de 6 PCIe 4.0
Rieles	Incluir, para montar en rack con sistema de administración de cables
Sistemas operativos certificados	Microsoft Windows Server Microsoft Windows Server Hyper-V Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware Red Hat KVM Oracle Linux
Licencia de Sistema Operativo Incluida	Debe incluir el licenciamiento para todos los procesadores y cores de todos los servidores para el sistema operativo Windows Server 2022 Standard

Fuente poder / Ventiladores	2 fuentes poder Hot Plug redundantes de 800W. Ventiladores redundantes
Seguridad	Deberá tener la capacidad de detectar posibles intrusiones además de recuperar el firmware de forma segura. Deberá poder comprobar el firmware como mínimo cada 24 horas verificando la validez y fiabilidad del firmware del sistema.
Gestión & Administración	Debe permitir el acceso de hasta tres sesiones en simultáneo Administración y monitoreo a través de un procesador de servicio dedicado, con el siguiente alcance: KVM (Keyboard, Video, Mouse) local y/o remoto Media (CD, USB) local y/o remoto. Consola de administración centralizada, que permita ver de manera gráfica el funcionamiento de todos los componentes internos del módulo de cómputo. Acceso vía Browser y línea de comandos. Debe soportar análisis predictivo de fallas mínimas sobre procesadores, memorias y discos de los módulos de cómputo. Se debe poder desplegar múltiples sistemas operativos en los módulos de cómputo simultáneamente y también poderse programar el despliegue a medida. Configurar el hardware y cambiar ajustes del sistema, tales como nivel del RAID, antes del despliegue del sistema operativo. También se debe tener la capacidad de capturar los ajustes del hardware y de desplegarlos a otros módulos de cómputo. Contar con una plataforma de análisis predictivo que brinde inteligencia con capacidad de predecir y prevenir problemas de infraestructura antes de que sucedan, a través de herramientas de predicción inteligentes como machine learning y/o inteligencia artificial.
Garantía	Debe ser brindada directamente por el fabricante, acorde a los procedimientos y políticas establecidos por la subsidiaria del fabricante en Perú.
	Debe cubrir fallas o defectos de fabricación, que puedan manifestarse durante su uso normal y en las condiciones imperantes.
	Debe ser por el periodo de 05 años, 24x7, el cual incluye reparación o de ser el caso sustitución del componente o total de componentes ofertados.
SOFTWARE DE BACKUP	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Características Generales	No debe estar catalogado como descontinuado o “end of life” o “end of sale”, deberá estar vigente tecnológicamente, pertenecer a la última versión o generación liberada por el

	fabricante a la fecha de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, mediante documentación oficial del fabricante con referencia al presente proceso.
Cantidad	Licenciamiento para 100 servidores virtuales y/o físicos; el cual también permita realizar el backup de las carpetas o archivos de servidores virtuales, estas licencias deberán ser en modalidad perpetua.
Operaciones de respaldo en entorno virtual	
Respaldo basado en snapshots de VMs VMware y Hyper-V	La solución debe proporcionar una copia de seguridad eficiente 'incremental para siempre' e incluir opciones de copias de seguridad completas y ad-hoc.
	La solución debe admitir la copia de seguridad de VM directamente desde SAN.
	La solución debería detectar automáticamente las máquinas virtuales con el uso compartido de bus SCSI y excluirlas de la copia de seguridad.
	La solución debería detectar automáticamente el espacio libre del datastore productivo y evitar el snapshot de copia de seguridad si el espacio está por debajo del umbral definido.
	La solución debería monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.
	La solución debería detectar automáticamente los snapshots de VMware huérfanas y eliminarlas.
	La solución debería permitir la exclusión de discos de máquinas virtuales y archivos de intercambio (swap) en copias de seguridad basadas en snapshots.
	La solución debería permitir la exclusión de archivos y carpetas de la copia de seguridad basada en snapshots.
	La solución deberá permitir la exclusión de los bloques marcados como eliminados para reducir el tamaño de la copia de seguridad y aumentar el rendimiento del respaldo.
	La solución no debería requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la recuperación granular.
	La solución no debe necesitar realizar copias de seguridad de sistema operativo separadas de las copias de seguridad de datos de la aplicación en máquinas virtuales para facilitar la recuperación granular de elementos de la aplicación.
	La copia de seguridad sin agente de máquinas virtuales debe truncar los registros de transacciones o archivos de Microsoft SQL, Microsoft Exchange y Oracle Database.
	La copia de seguridad sin agente de máquinas virtuales debe proporcionar copias de seguridad de registros o archivos de

	transacciones de Microsoft SQL, Oracle Database y PostgreSQL junto con copias de seguridad basadas en snapshots.
	La solución debería permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes o plugins en Máquinas Virtuales.
Respaldo de VMware con integraciones de snapshot de almacenamiento	La solución debe integrarse con los sistemas de almacenamiento y utilizar snapshots de almacenamiento para las operaciones de respaldo.
	La solución debería poder leer los datos de la máquina virtual directamente desde un snapshot de almacenamiento a través de una conexión SAN.
	La solución deberá proporcionar la capacidad de explorar máquinas virtuales en snapshots de almacenamiento y recuperar instantáneamente la máquina virtual, el archivo del sistema operativo o la carpeta o los elementos de la aplicación directamente desde el snapshot de almacenamiento. Esta capacidad también debería aplicarse a los snapshots de almacenamiento creados independientemente de la aplicación de respaldo.
	La solución deberá poder utilizar snapshots de almacenamiento para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.
Protección de datos continua para VMware (CDP)	Para eliminar el tiempo de inactividad y minimizar la perdida de datos de VMware vSphere, se debe incorporar una solución de protección continua de datos, logrando RTOs y RPOs mínimos para cargas de trabajo críticas.
	La solución deberá replicar máquinas virtuales sin snapshots del ambiente virtual y debe capturar todas las E/S de escritura directamente del disco de la VM.
	La solución no deberá tener dependencia de hardware y deberá proteger cualquier S.O. y Aplicación que corra en una VM de vSphere, sin importar si se ejecuta en infraestructuras convergentes, hiperconvergentes o discos locales del vSphere ESXi.
	La solución deberá ser una replicación asíncrona que se pueda utilizar sin limitación de distancia.
	La funcionalidad deberá estar incluida en el mismo licenciamiento de respaldo, es decir que no debe requerir alguna otra licencia adicional.
Operaciones de respaldo, entornos físicos	
Respaldo basado en agente de entornos físicos	La solución debe admitir copias de seguridad físicas de sistemas operativos Windows, Linux, UNIX y MAC.
	La solución debería facilitar la copia de seguridad a nivel de imagen y de archivo de entornos físicos o basados en la nube.

	La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.
	La solución debe admitir la copia de seguridad de los servidores de Windows configurados como clúster.
	La solución debe proporcionar complementos de respaldo para las aplicaciones MS SQL, Oracle RMAN y SAP HANA, permitiendo la centralización de repositorio.
	La solución debe proporcionar conocimiento de la aplicación al realizar copias de seguridad de MySQL y PostgreSQL que se ejecutan en Linux.
	La solución debe permitir mover los archivos de respaldo entre cualquier tipo de repositorio de respaldo (aun cuando el repositorio destino sea de un tipo distinto al del origen) sin necesidad de usar la gestión regular de archivos (copiar/pegar).
	La solución debe permitir mover los respaldos entre las tareas y copiar los respaldos entre repositorios.
Operaciones de recuperación	
Recuperación de VMs VMware \ Hyper-V y servidores físicos	La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo propietario y no debe depender de ninguna infraestructura de respaldo como, por ejemplo, el catálogo central, para la recuperación.
	La solución debe proporcionar tecnología de recuperación de la máquina virtual snapshot, correr múltiples Virtual Machine directamente desde el servidor de copia de seguridad del repositorio.
	La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales VMware, Hyper-V y Nutanix AHV.
	La solución debe permitir que las copias de seguridad de máquinas virtuales en la nube puedan ser restauradas en cualquier nube pública o volver a una máquina virtual en un hipervisor local en las instalaciones.
	La solución debería permitir la recuperación de VMware Virtual Machine a través del canal de fibra SAN.
	La solución debe escanear los datos de la máquina virtual con un software antivirus antes de restaurar la máquina al entorno de producción. La solución debería abortar la operación de recuperación si se detecta malware.
	La solución debería proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script en el sistema operativo invitado que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.

	La solución debería proporcionar una recuperación completa de la copia de seguridad basada en el Agente con la capacidad de crear un medio de arranque para el servidor específico, del tipo bare metal.
	La solución debe permitir la recuperación instantánea de copias de seguridad basadas en agentes para VMware o máquinas virtuales Hyper-V.
	La solución debe permitir la recuperación instantánea de copias de seguridad de sistemas de archivos tipo NAS (FileShares).
	La solución debería facilitar la recuperación de VMware o una copia de seguridad basada en agentes directamente en Google Platform, Amazon AWS o Microsoft Azure y Microsoft Azure Stack.
	La solución debería convertir automáticamente UEFI a BIOS durante la operación de recuperación de Amazon AWS.
Recuperación a nivel de archivo	La solución debería facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente o plugin de recuperación en un servidor virtual o físico.
	La solución debería poder recuperar archivos en un sistema operativo invitado de máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.
	La solución debe permitir delegar operaciones de restauración y proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de buscar máquinas, recursos compartidos de archivos y archivos específicos en todas las copias de seguridad.
	La solución debe admitir todos los sistemas de archivos dentro del alcance en la Institución.
	La solución debe permitir restaurar las listas de control de acceso (ACL) de archivos y carpetas sin la necesidad de sobre escribir los archivos.
Recuperación de elementos de aplicación	La solución debería admitir la recuperación granular de las aplicaciones de Microsoft Active Directory, Exchange, SQL, SharePoint y PostgreSQL.
	La solución debería admitir la recuperación granular de bases de datos Oracle a partir de copias de seguridad basadas en imágenes u Oracle RMAN.
	La solución no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.
	La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de examinar y recuperar elementos de Microsoft Exchange y bases de datos SQL u Oracle.

	La solución debe permitir la recuperación instantánea de base de datos SQL u Oracle desde la copia de seguridad al último estado o a un punto anterior en el tiempo a cualquier servidor de base de datos de producción o clúster (físico o virtual) en minutos, independientemente de su tamaño.
Requisitos de la solución de respaldo	
Copia de seguridad en disco	La solución debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.
	La solución debe ser independiente del almacenamiento y debe contar con tecnología integrada de deduplicación y compresión.
	La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado.
	La solución debe poder escalar tanto horizontal como verticalmente.
	La solución debe proporcionar un mecanismo fácil para expandir o contratar el almacenamiento de respaldo de destino.
	La solución debería ofrecer la flexibilidad para ajustar el tamaño del bloque de deduplicación de datos y el nivel de compresión de datos.
	La solución debe integrarse con los dispositivos de deduplicación EMC Data Domain, HPE Store Once, Quantum, ExaGrid, Fujitsu e Infinidat.
Copia de seguridad en cinta	La solución debería admitir de forma nativa la copia del respaldo a cinta y no debería requerir software adicional para su administración.
	La solución debe admitir copias de seguridad deduplicadas y comprimidas en medios de cinta.
	La solución debe admitir medios de cinta WORM.
	La solución no debe requerir licenciamiento adicional para el uso de librerías sin importar la cantidad de drives que tengan.
Repositorio y Copia de seguridad en la nube	La solución debería admitir de forma nativa como repositorio y el traslado de archivos de respaldo a Amazon S3 (con inmutabilidad), IBM Cloud Object Storage, Azure Blob Cloud Storage (con inmutabilidad), Google Cloud Storage, y otras plataformas de almacenamiento en la nube compatibles con S3.
	La solución debería admitir de forma nativa el traslado de archivos de respaldo a Amazon S3 Glacier (incluido Deep

	Archive) con capacidad de inmutabilidad, y Microsoft Azure Blob Storage Archive Tier para archivado a largo plazo de copias de seguridad.
	La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.
	La solución debe proporcionar soporte para el almacenamiento de objetos en las instalaciones.
	La solución debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
	La solución debería ofrecer inmutabilidad en el almacenamiento de objetos S3 a nivel de depósito.
	La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. Idealmente, ambas opciones se pueden combinar.
Seguridad de datos de respaldo	La solución debería encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.
	La solución debe proporcionar un cifrado AES de 256 bits con tecnología de protección de pérdida de contraseña, por lo que los datos se pueden descifrar si se pierde la contraseña operativa.
	Todos los componentes de la solución de respaldo deben admitir autenticación Kerberos.
	La solución debe integrarse con autenticación de credenciales del tipo gMSA.
	La solución debe permitir autenticación multifactor (MFA) para una verificación adicional de usuario en la consola de administración de la solución.
	La solución debe integrarse con SAML 2.0 para la autenticación extendida.
	La solución debe proporcionar control de acceso basado en roles a través de una interfaz de usuario web para la mayoría de las operaciones de recuperación y respaldo.
Verificación de datos de respaldo	La solución debería leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debería reconstruir automáticamente el bloque dañado con datos de producción.
	La solución deberá iniciar automáticamente las máquinas virtuales de VMware y Hyper-V Windows y Linux así como de agentes de nube y físicas a partir de copias de seguridad y verificar el sistema operativo y la disponibilidad de la aplicación. Esta prueba no debe tener impacto en la red de

	producción. La solución debe proporcionar un informe de verificación de recuperación.
	La solución debería escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.
Otros requerimientos	La solución debe proporcionar la tecnología de migración de máquina virtual VMware donde la máquina virtual se puede migrar a través de clústeres y centros de datos de VMware y entre centros de datos físicos.
	La solución debería poder utilizar la copia de seguridad o réplica de la máquina virtual para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.
	La solución debe presentar la tecnología de replicación de máquina virtual VMware con la capacidad de configurar el failover y el failback, convertir en tiempo real el tipo de disco de la máquina virtual de thin a thick y viceversa y deshacer la operación de recuperación de fallas o recuperación de fallas, incluido en la licencia de respaldo y misma consola.
	La solución debe incluir un mecanismo de copia de seguridad fuera del sitio con la capacidad de seleccionar individualmente los conjuntos de copias de seguridad que deben copiarse y definir una retención diferente de las copias de seguridad en el almacenamiento secundario de copias de seguridad.
	La solución debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de limitar la utilización del ancho de banda.
Copia de seguridad NAS	La solución debe proporcionar una copia de seguridad eficiente basada en archivos incrementales.
	La solución debe admitir recursos compartidos de archivos basados en NFS, SMB, Windows y Linux.
	La solución debe aprovechar los snapshots basadas en matrices para copias de seguridad basadas en archivos siempre que sea posible.
	La solución debe aprovechar los snapshots de VSS cuando sea posible.
	La solución debe proporcionar una recuperación incremental a cualquier plataforma objetivo-heterogénea.
	La solución debe proporcionar un mecanismo de reversión incremental para cualquier recurso compartido NAS.
	La solución debe proporcionar la capacidad de archivo granular de archivos, archivando tipos de archivos específicos.
Operaciones de respaldo en entorno nube	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos

	Amazon Elastic Compute Cloud (EC2), Amazon Relational Database Service (RDS) y Amazon Elastic File System (EFS). También debe permitir respaldar y restaurar las configuraciones de Amazon Virtual Private Cloud (VPC).
	La solución debe poder realizar las siguientes operaciones de protección de datos: crear instantáneas nativas de la nube de instancias EC2, crear instantáneas nativas de la nube de los recursos de RDS, crear copias de seguridad a nivel de imagen de instancias EC2 y crear copias de seguridad de los sistemas de archivos EFS.
	La solución debe poder realizar las siguientes operaciones de recuperación de datos respaldados: restaurar instancias EC2 completas, restaurar volúmenes de instancias EC2, restaurar archivos y carpetas de instancia EC2, restaurar instancias de base de datos de RDS, restaurar sistemas de archivos EFS completos, así como archivos y directorios EFS, configuraciones completas y elementos específicos de configuraciones de VPC.
	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Microsoft Azure.
	La solución de poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de máquinas virtuales de Azure, crear copias de seguridad a nivel de imagen de las bases de datos de Azure SQL, crear instantáneas nativas en la nube de recursos compartidos de archivos de Azure, restaurar archivos individuales de recursos compartidos de archivos de Azure, bases de datos específicas de Azure SQL, máquinas virtuales de Azure completas, discos virtuales individuales y archivos y carpetas del sistema operativo invitado.
	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Google Cloud.
	La solución de poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de instancias de máquinas virtuales de Google, crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de las instancias de Google Cloud SQL, restaurar instancias de Google Cloud SQL completas, bases de datos de Google Cloud SQL específicas, instancias de máquinas virtuales de Google completas, discos persistentes individuales y archivos y carpetas del sistema operativo invitado.
Monitoreo y Reporting de Respaldo	La Institución requiere informes y monitoreo precisos de la infraestructura de respaldo y el estado del trabajo para

	garantizar que se puedan cumplir los objetivos de recuperación.
	La solución debe proporcionar información del estado de protección de cargas de trabajo virtuales, físicas o basadas en nube.
	La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo.
	La solución debe alertar por adelantado si el objetivo de la copia de seguridad se acerca a la capacidad.
	La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento, y el proveedor debe actualizar dinámicamente la detección.
	La solución debe proporcionar un informe de evaluación de Infraestructura VMware para asegurar que el entorno esté preparado para las operaciones de respaldo basadas en snapshots y detectar máquinas virtuales que requieren implementación de respaldo basada en agente.
	La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.
	La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas.
	La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.
	La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.
	La solución debe proporcionar una infraestructura de respaldo y un informe de cambios de política para fines de auditoría.
	La solución debe permitir definir dashboards de monitoreo personalizados e integraciones con sistemas ITSM con la ayuda de REST APIs.
	La solución debe permitir programar la entrega automática de dashboards, informes y carpetas de informes. Se debe poder optar por recibir dashboards e informes por correo electrónico, guardar dashboards e informes en una carpeta local o recurso compartido de red.
	La solución debe notificar a los usuarios sobre eventos importantes, cambios y posibles problemas en el entorno virtual y de copia de respaldo.

	La solución debe ser capaz de tomar acciones de remediación como por ejemplo ejecutar un script que encienda una VM, o ejecutar un script que agregue una VM a un trabajo de respaldo existente o ejecutar un script que elimine el último snpashot en VMware o que elimine el último checkpoint en HyperV.
Respaldo de Nutanix AHV	La solución debe admitir la copia de seguridad a nivel de imagen sin agente de las máquinas virtuales Nutanix AHV.
	La solución debe admitir copias de seguridad utilizando las snapshots nativas de Nutanix para copias de seguridad frecuentes y rápidas.
	La solución debería permitir la recuperación de cualquier carga de trabajo en la máquina virtual Nutanix AHV.
	La solución debe admitir la recuperación granular sin agente de archivos y elementos de aplicaciones desde la copia de seguridad a nivel de imagen.
	La solución debe permitir la recuperación snapshot de máquinas desde el respaldo.
Garantía y Soporte	Debe ser brindada directamente por el fabricante, acorde a los procedimientos y políticas establecidos por la subsidiaria del fabricante en Perú.
	Debe incluir parches y derecho a actualizaciones a últimas versiones estables y liberadas por el fabricante.
	Debe ser por el periodo de 05 años, 24x7.
PLATAFORMA PARA GESTIÓN DE RIESGOS CIBERNÉTICOS	
DESCRIPCIÓN	
Deberá poder implementarse y gobernar los host de tipo servidores incluyendo los activos que contengan estos hosts, por el periodo de cinco (05) años.	
No debe estar catalogado como descontinuado o “end of life” o “end of sale”, deberá estar vigente tecnológicamente, pertenecer a la última versión o generación liberada por el fabricante a la fecha de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, mediante documentación oficial del fabricante con referencia al presente proceso.	
Deberá contar con una consola de administración centralizada que incluya todos los criterios de seguridad de acceso como factor de doble autenticación; además de estar diseñada y acondicionada para el gobierno remoto en tiempo real, de equipos dentro y fuera de la red de la entidad.	
Deberá integrar un inicio de sesión único (SSO) para una autenticación segura y sin problemas en base a SAML V2, admitiendo la integración con todos los proveedores de identidad compatibles con SAML v2, incluidos PingID, PingFederate, AWS, Azure, Auth0 y Okta.	
Deberá ser compatible con proveedores adicionales de autenticación multifactor (MFA) como ID de ping, Okta y Aplicaciones TOTP Authenticator.	
Deberá poder habilitar el acceso a usuarios basados en roles, administrador con acceso total, supervisor con posibilidad de solo ver el desempeño de la solución con posibilidad de generar informes y usuarios con privilegios restringidos a determinados módulos.	
Deberá poder integrarse al directorio activo a fin de descubrir, desplegar e integrar el sistema a la red de la entidad.	

Debe poder enviar alertas que se envíen automáticamente al correo electrónico cuando se detecte una vulnerabilidad con calificación crítica y/o alta y/o media y/o baja, cuando se determine la viabilidad de determinado ataque o malware reconocido, cuando Se detecte una configuración débil o errónea se presente, cuando se presente un indicador de compromiso, la alerta deberá asociarse al ataque o malware especifico, cuando se presente un indicador de ataque, cuando se realice una determinada acción de respuesta no logre mitigar un ataque.
Deberá poder lanzar tareas de escaneo de red desde los nodos que cuenten con el agente de gestión.
Deberá incluir sistema de gestión de riesgos y usuarios desde donde se pueda habilitar perfiles de acceso con privilegios para ver, ver y editar configuraciones y ver, editar y lanzar tareas de remediación.
Deberá contar con un sistema de auditoría que identifique mediante código determinado Jobs ejecutado, fecha y hora de ejecución, además del usuario responsable de la ejecución.
Deberá presentar un panel de resumen de la actividad de los activos donde se pueda apreciar mínimamente: Nombre del host, IP, Dirección MAC, Sistema Operativo, Versión y/o detalle técnico del agente que lo gobierna, Grupo al que pertenece, Status de actividad del servicio, Consumo en tiempo real del CPU, Consumo en tiempo real de la memoria RAM, Consumo en tiempo real de la red, Consumo en tiempo real de la actividad del disco.
Deberá ser compatible con los siguientes sistemas operativos actuales o superiores a Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows 10, Microsoft Windows 11, Apple MacOS X 10.10 y Apple MacOS X 10.11, Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 18.10, Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.10, Debian 7, Debian 8, Debian 9, Debian 10, Amazon Linux, Amazon Linux 2, Redhat Enterprise Linux 5, Redhat Enterprise Linux 6, Redhat Enterprise Linux 7, Redhat Enterprise Linux 8, CentOS 5, CentOS 6, CentOS 7, CentOS 8, Oracle Linux 5, Oracle Linux 6, Oracle Linux 7, Oracle Linux 8, Fedora 27, Fedora 28, Fedora 29, Fedora 31, Fedora 32.
Deberá integrar componentes de ciberseguridad que contribuyan a la gestión transversal de un proceso de ciberseguridad para estaciones de trabajo y servidores independiente del sistema operativo.
Deberá gestionar servidores y estaciones de trabajo multiplataforma a través de la ejecución de un agente ligero instalado en cada activo, el agente debe ser de un tamaño máximo de 20 MB.
Deberá garantizar que la instalación del agente no demande reinicios ni impacte en el consumo recursos durante su etapa de diagnóstico.
Deberá integrar su propia fuente de inteligencia de vulnerabilidades la cual deberá realizar mínimamente 150,000 comprobaciones.
Deberá poder realizar escaneos rápidos de 5 a 7 minutos para detectar vulnerabilidades y riesgos automatizando todas las tareas desde una sola consola.
Deberá poder instalar agentes en puntos finales heterogéneos y realizar todas las tareas que se les asignan sin consumir ancho de banda ni recursos del sistema excesivos.
Deberá poder supervisar y administrar los dispositivos distribuidos desde una consola centralizada logrando incorporar nuevos dispositivos con facilidad y escalar a cualquier número de dispositivos.
Deberá integrar un módulo de gestión de vulnerabilidades capaz de detener infracciones de seguridad identificando automáticamente las vulnerabilidades críticas, evaluando los riesgos y el

potencial de explotación, priorizando las vulnerabilidades cruciales en función de su gravedad y corrigiéndolas instantáneamente mediante parches.
Deberá detectar el Common Vulnerability Scoring System (CVSS), que determina la gravedad de la vulnerabilidad en función de las características principales que se traducen en una puntuación numérica.
Deberá priorizar vulnerabilidades considerando factores internos y externos influyen en el panorama de amenazas en vivo en toda la organización llevando más allá de las herramientas que solo muestran puntajes CVSS considerando la actividad de explotación, el tiempo y la importancia de los sistemas afectados presentando mínimamente esta clasificación: Vulnerabilidades de movimiento lateral refiriéndose a vulnerabilidades que se extienden a la red a medida que la amenaza se mueve de un dispositivo a otro y de un activo a otro, permitiendo que los atacantes recopilen datos valiosos, Vulnerabilidades fácilmente explotables que refieren a vulnerabilidades que son conocidas en el dominio público, lo que hace que un exploit se configure fácilmente, Vulnerabilidades de explotación pública disponible que hace referencia a vulnerabilidades para las cuales las explotaciones están disponibles públicamente y que se han producido en el pasado y Vulnerabilidades explotables en la red que refieren a vulnerabilidades que pueden explotarse con acceso a la red, a menudo de forma remota. El camino del atacante es a través de la capa de red.
Deberá poder generar informes que enumeren los detalles de las vulnerabilidades según los grupos de dispositivos y dispositivos específicos, el reporte debe incluir las instancias de vulnerabilidades para cada activo vulnerable y una descripción de cada vulnerabilidad.
Deberá poder reconocer las vulnerabilidades de cada grupo y host para posteriormente clasificar por gravedad, l gravedad de las vulnerabilidades se representa mediante códigos de color Rojo – Crítico, Naranja – Alto, Amarillo – Medio, Verde – Bajo.
Deberá poder agrupar de forma gráfica los hosts, los activos implicados y las vulnerabilidades debidamente clasificadas con el correspondiente status del servicio.
Deberá poder organizar de forma sencilla graficas de host más afectados a fin de tomar atención y priorizar las tareas de remediación.
Deberá incluir una descripción detallada de las tareas de remediación o FIX por cada vulnerabilidad detectada y ponderarla.
Deberá poder mostrar un panel que agrupe las vulnerabilidades por los kits de explotación que se pueden utilizar para explotar la debilidad como por ejemplo Zyklon Backdoor, ZombieLoad, VegaLocker Ransomware, Underminer Exploit Kit, ThreadKit Exploit Kit, Sundown-Pirate Exploit Kit. Esto permitiría priorizar las tareas de remediación.
Deberá permitir implementar políticas de exclusión de vulnerabilidades de los informes, logrando excluir/eliminar vulnerabilidades de los informes después de aceptar los criterios de riesgo de exclusión. La política de exclusión se puede aplicar para una sola vulnerabilidad, varias vulnerabilidades o todas las vulnerabilidades de un activo.
Deberá permitir implementar políticas de exclusión de parches de ser considerado para un trabajo de aplicación de parches o una regla logrando configurar una política para toda la cuenta para excluir el parche de la lista mientras crea un trabajo de aplicación de parches o una regla. Si no se aprueba un parche o si desea evitar las actualizaciones del sistema operativo o del paquete de servicio, o si hay herramientas de desarrollo que no desea actualizar, se puede aplicar una política de exclusión.
Deberá automatizar el proceso de gestión de vulnerabilidades.

Deberá integrar un módulo de gestión de cumplimiento capaz de reforzar las configuraciones del sistema para reducir la exposición a amenazas, a través del cumplimiento de estándares regulatorios populares de la industria, como HIPAA, PCI, ISO y NIST.
Deberá poder escanear de forma remota cualquier punto final vulnerable o desviado para remediar el riesgo de manera proactiva.
Deberá poder presentar gráficos de cumplimiento por plataforma evaluada.
Deberá poder crear plantillas personalizadas de auditoría de cumplimiento, definiendo y automatizando la validación de condiciones específicas de cumplimiento.
Deberá poder validar como mínimo 3 aspectos de cumplimiento: Cumplimiento predeterminado, brindando la capacidad de que cada sistema operativo tenga reglas individuales de forma predeterminada, la solución deberá asignar los valores, Cumplimiento genérico, diseñado para corresponder a los diferentes sistemas operativos y configuraciones de seguridad, como la política de bloqueo de cuentas, las plantillas administrativas, los tipos de autenticación, etc., Cumplimiento normativo define estándares, como los estándares PCI, HIPAA y NIST.
Deberá poder presentar de forma gráfica la cantidad y el detalle de las configuraciones de seguridad no habilitadas en cada host evaluado.
Deberá cubrir mínimamente la siguiente lista de puntos de referencia para su módulo de cumplimiento: • Tiempo mínimo de la contraseña • Permitir estados de espera cuando el equipo o servidor inicio sesión • Requerir una contraseña cuando una computadora se activa • Criptografía del sistema para el forzado de una fuerte protección de claves para las claves de usuario almacenadas en la computadora • La clave debe cumplir los requerimientos de complejidad • Desactivar la prevención de ejecución de datos para el ejecutable de ayuda HTML • Requerir contraseña al conectarse • Habilitar la autenticación del cliente del asignador de extremos de RPC • Requerir autenticación de usuario para conexiones remotas mediante autenticación de nivel de red • Requerir el uso de inicio rápido • Desactivar la prevención de ejecución de datos para Explorer • Hacer cumplir el historial de contraseñas • Seguridad de la red: nivel de autenticación de LAN Manager • Control del comportamiento del Registro de eventos cuando el archivo de registro alcanza su tamaño máximo (Seguridad) • Inicio de sesión interactivo: límite de inactividad de la máquina • Desactiva las notificaciones de aplicaciones en la pantalla de bloqueo • Permitir el acceso remoto a la interfaz Plug and Play • No procesar la lista de ejecutar una vez para la configuración del equipo • Restablecer contador de bloqueo de cuenta después • No enumerar usuarios conectados en equipos unidos a un dominio • Umbral de bloqueo de cuenta • Seguridad de red: seguridad de sesión mínima para clientes basados en NTLM SSP (incluido RPC seguro)

• Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM • No procesar la lista de ejecución heredada para la configuración del equipo • Impedir la instalación de dispositivos extraíbles • Longitud mínima de la contraseña • Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash y la firma • Control de cuentas de usuario: eleve solo las aplicaciones de UIAccess que están instaladas en ubicaciones seguras • Acceso a la red: rutas y subrutas de registro accesibles de forma remota • Miembro del dominio: cifre o firme digitalmente los datos del canal seguro (siempre) • Control de cuentas de usuario: Comportamiento del aviso de elevación para usuarios estándar • Control de cuentas de usuario: detecte instalaciones de aplicaciones y solicite la elevación • Cuentas: estado de la cuenta de invitado • Acceso a la red: restrinja el acceso anónimo a canalizaciones con nombre y recursos compartidos • Acceso a la red: no permitir la enumeración anónima de cuentas SAM • Acceso a la red: permite que los permisos de Todos se apliquen a usuarios anónimos • Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador • Control de cuentas de usuario: eleve solo los ejecutables que estén firmados y validados
Deberá auditar el cumplimiento a través de rutinas para presentar y/o evidenciar siempre una foto del momento, permitiendo evaluar estadísticamente el fortalecimiento de las configuraciones.
Deberá integrar un módulo de gestión de activos para inventariar el hardware y el software relacionado al activo con información detallada de IP, MAC, Plataforma de Sistema Operativo, Detalles de Discos, Detalle de Componentes, fabricantes y el estado del activo.
Deberá integrar un módulo de gestión de activos que presente gráficamente la distribución de dispositivos.
Deberá integrar un módulo de gestión de activos que clasifique los inventarios en tiempo real en tipos de dispositivos, por fabricante, por riesgo asociado, por licencias, por aplicaciones, por violaciones a las políticas de uso, por uso de aplicaciones inscritas como lista negra, como lista blanca y aplicaciones poco utilizadas.
Deberá integrar un módulo de gestión de activos que integre alertas y genere informes automáticos de forma centralizada.
Deberá integrar un módulo que proporcione una visibilidad total sobre los puntos finales gestionados.
Deberá integrar un módulo que ejecute acciones integradas que ayuden a que los terminales cumplan con las normas y estén actualizados con parches de software y hardware.
Deberá integrar un módulo que ejecute acciones para alinear políticas de uso de los activos tales como: • Bloquear una aplicación por determinado tiempo • Permitir la ejecución de aplicaciones en determinados intervalos de tiempo

• Bloquear y determinar el acceso a dispositivos por determinado intervalo de tiempo • Enviar un script • Gestionar un proceso • Gestionar un servicio • Gestionar un registro • Instalar o desinstalar una aplicación • Evaluar la red • Evaluar la transferencia de archivos • Validar que programas inician sesión • Borrar un archivo • Mover un archivo a cuarentena
Deberá integrar un módulo de consultas y respuestas que detecten ataques actuales y en curso incluyendo comandos para responder a las amenazas.
Deberá ser compatible con las fuentes STIX/TAXII, OpenIOC y Yara y use inteligencia de amenazas de otras fuentes para detectar indicadores de compromiso (IoC).
Deberá contar con su propia fuente de amenazas, los feeds de amenazas deben estar en formato JSON y se deberá poder realizar comprobaciones de registros y archivos y comprobaciones md5sum para fuentes de amenazas.
Deberá agregar y administrar diferentes fuentes de amenazas las cuales deben estar en constante actualización.
Deberá poder ejecutar consultas basadas en síntomas de ataque para investigar comportamientos anormales o detectar un ataque en curso en la red.
Deberá reconocer mínimamente los siguientes indicadores de ataque (IoA): • Notificación de AntiVirus Security Center deshabilitada • Anomalías en la creación de cuentas de computadora • Cortafuegos deshabilitados • Notificación del centro de seguridad del cortafuego deshabilitada • Procesos Altamente Sospechosos • Ejecutable de Svchost altamente sospechoso • Detección de ataques ICMP DoS • Detección de ataques de reproducción de Kerberos • Acceso al registro deshabilitado • Anomalías de tareas programadas • Explorador sospechoso • Proceso sospechoso llamado operación de servicio de sistema privilegiado • Anomalías de instalación de servicio sospechosas • Inicio de sesión de grupo especial sospechoso • Registro sospechoso de auditoría de seguridad de Windows borrado • Sistema ASLR deshabilitado • Sistema DEP siempre apagado • Sistema ExecShield deshabilitado • GateKeeper del sistema deshabilitado • Sistema NX DX deshabilitado • UAC del sistema desactivado • Administrador de tareas deshabilitado

• Notificación del centro de seguridad de UAC deshabilitado • Aplicación no autorizada que accede al puerto LPC • Actualizaciones Notificación del centro de seguridad deshabilitada • Anomalías en la creación de cuentas de usuario • Cuenta de usuario bloqueada o desbloqueada • Anomalías fallidas en el inicio de sesión de la cuenta de usuario • Cuenta de usuario o computadora creada o eliminada • Uso de CPU o RAM de Windows Más del 95 Porcentaje • Filtrado de Windows Bloqueado Conexión de paquetes sospechosos • Firewall de Windows no se pudo inicializar o iniciar
Deberá poder crear su propio grupo de consultas y respuestas especificando un nombre de paquete, la cantidad de veces que desea ejecutar la consulta y los intervalos en los que desea ejecutarla.
Deberá poder personalizar la ejecución de consultas inmediatamente, diariamente, semanalmente, mensualmente o en una fecha específica, especificando la hora y los días correspondientes de la semana, mes o fecha determinando la gravedad la cual puede ser baja, media, alta o crítica de la consulta.
Deberá integrar un módulo de gestión de parches el cual permita relacionar sus actividades con los demás servicios requeridos.
Deberá permitir aplicar parches de seguridad que tengan por objetivo principal eliminar vulnerabilidades en el software por lo que sus gráficas y reportes estarán alineados a medir el impacto en términos de seguridad.
Deberá integrar un sistema de parchado, que automatice las tareas de parcheo de extremo a extremo, desde el escaneo hasta la implementación, para reducir la superficie de ataque y mejorar la postura de seguridad de manera efectiva.
Deberá incluir parches para todos los principales sistemas operativos, como Windows, Mac, Linux, firmware y muchas aplicaciones de terceros.
Deberá poder relacionar los parches que se aplican con las vulnerabilidades latentes y llevar un control estadístico de la aplicación e impacto de estos.
Deberá poder controlar el proceso de parchado considerando mínimamente: Control sobre el reinicio, Remediación final o definitiva de una vulnerabilidad, Notificar la aplicación del parche, Lanzar un script de remediación antes y después de la aplicación del parche, Testear y desplegar
Deberá cubrir la aplicación de parches software de terceros.
Deberá poder escanear vulnerabilidades a dispositivos de red, páginas web y URLs específicos desde cualquier equipo o servidor con el agente.
Deberá incluir rutinas de troubleshooting para ejecutarse remotamente.
Deberá poder actualizar cualquier firma de antivirus de forma centralizada permitiendo corregir debilidades en las configuraciones.
Deberá poder mapear amenazas de real-time threat hunting.
Deberá permitir generar informes por cada módulo con los resultados estadísticos en el tiempo personalizando los informes de acuerdo con los requerimientos de la entidad.
Deberá poder generar reportes para el módulo de gestión de vulnerabilidades presentando mínimamente: • Todas las vulnerabilidades • Dispositivos monitoreados actualmente

- Tendencia de vulnerabilidades existentes y nuevas
- Ataques de alta fidelidad
- Activos afectados (vulnerabilidades)
- Hosts afectados (vulnerabilidades)
- Tendencia de vulnerabilidades mitigadas
- Nueva tendencia de vulnerabilidades
- Hosts no vulnerables
- Estadísticas de parches
- Vulnerabilidades descubiertas recientemente
- Las 10 principales vulnerabilidades altamente explotadas
- Las 10 soluciones recomendadas principales
- Las 10 principales vulnerabilidades en los hosts
- Las 10 principales vulnerabilidades por puntaje CVSS
- Los 10 principales hosts vulnerables
- Informe diario de vulnerabilidades
- Informe Mensual de Vulnerabilidades
- Informe Trimestral de Vulnerabilidades
- Informe Semestral de Vulnerabilidades
- Tendencia de vulnerabilidades
- Gráfico de envejecimiento de la vulnerabilidad
- Recuento de vulnerabilidades basado en el grupo
- Recuento de vulnerabilidades basado en la familia del sistema operativo
- Recuento de vulnerabilidades basado en el sistema operativo
- Métricas de vulnerabilidad
- Estadísticas de mitigación de vulnerabilidades
- Gráfico de estadísticas de mitigación de vulnerabilidades
- Estadísticas de puntuación de vulnerabilidad
- Métricas de gravedad de vulnerabilidad
- Gráfico de estadísticas de vulnerabilidad
- Vulnerabilidad basada en CVSS

La solución de gestión de riesgo cibernético deberá poder generar reportes para el módulo de gestión de cumplimiento presentando mínimamente:

- Todos los puntos de referencia
- Desviaciones de referencia por dispositivos
- Desviaciones de referencia por grupo
- Desviaciones comparativas por sistema operativo
- Informe de referencia
- Puntos de referencia Estadísticas de incumplimiento
- Punto de referencia de cumplimiento
- Estadísticas de cumplimiento por regla
- Dispositivos monitoreados actualmente
- Dispositivos con configuraciones incorrectas
- Tendencia de configuraciones incorrectas existentes y nuevas
- Tendencia de parches de configuración faltantes existentes y nuevos

• Correcciones de errores de configuración fallidos • Activos afectados (problemas de configuración) • Hosts afectados (problemas de configuración) • Informe diario de parches de configuración instalados • Informe mensual de parches de configuración instalados • Informe trimestral de parches de configuración instalados • Informe semestral de parches de configuración instalados • Informe semanal de parches de configuración instalados • Informe anual de parches de configuración instalados • Correcciones de errores de configuración instalados	
Garantía: Debe ser brindada directamente por el fabricante, acorde a los procedimientos y políticas establecidos por la subsidiaria del fabricante en Perú. Debe incluir parches y derecho a actualizaciones a últimas versiones estables y liberadas por el fabricante. Debe ser por el periodo de 05 años, 24x7.	
LIBRERÍA DE RESPALDO A CINTAS	
CARACTERÍSTICAS	**DESCRIPCIÓN**
Características Generales	Debe ser de propósito específico, donde todos sus componentes o partes deben ser de la misma marca; y, además, no se requiera de la instalación de software y/o hardware adicional que no forme parte del bien ofertado.
	Debe ser nuevo (de primer uso), no catalogado como descontinuado o “end of life” o “end of sale”, deberá estar vigente tecnológicamente, pertenecer a la última versión o generación liberada por el fabricante y ser fabricado en el año de la presentación de la propuesta. Se debe acreditar para la presentación de la propuesta, mediante documentación oficial de la subsidiaria del fabricante en Perú con referencia al presente proceso.
Tecnología	Ultrium LTO 9 – FC de 8 Gb
Capacidad	Deberá de soportar mínimo 8 slots
Drivers	(01) Drives Ultrium LTO 9
Cartuchos incluidos	(20) cartuchos LTO 9 de datos y (01) cartuchos de limpieza
Accesorios	Incluir cables de poder, cables FC de 5m. mínimo, kit de montaje para rack y funcionamiento de la solución.
Software de monitoreo	Deberá de incluir las siguientes características: • Mitigar los riesgos de errores de dispositivos, mediante el análisis de la probabilidad de fallos de dispositivos. • Planificar las futuras inversiones en hardware mejor mediante el análisis de los cuellos de botella en la utilización de la unidad / de la cinta. • El software deberá de generar reportes y graficar opciones para monitorear los indicadores clave de rendimiento, la salud y la utilización de unidades de cinta y cartuchos.

Garantía	Debe ser brindada directamente por el fabricante, acorde a los procedimientos y políticas establecidos por la subsidiaria del fabricante en Perú.
	Debe cubrir fallas o defectos de fabricación, que puedan manifestarse durante su uso normal y en las condiciones imperantes.
	Debe ser por el periodo de 05 años, 24x7, el cual incluye reparación o de ser el caso sustitución del componente o total de componentes ofertados.

3.2 COMPONENTE SOFTWARE

Este componente se encuentra conformado por los ítems:

ITEM	DESCRIPCIÓN	CANTIDAD
1	Software PACS, RIS y de Reconocimiento de Voz	1
2	Dictáfonos	6
3	Terminales VDI - Estaciones de Visualización	40
4	Terminales VDI - Estaciones de Diagnóstico	4
5	Pantallas de Visualización para Sala de Operaciones	3
6	Teclados Medico para Sala de Operaciones	3
7	Mouses Medico para Sala de Operaciones	3

3.2.1 ITEM 1: SOFTWARE PACS, RIS Y DE RECONOCIMIENTO DE VOZ

- **SUB-ITEM 1.1: SOFTWARE PACS**

La solución debe contar con garantía de 05 años y licencia perpetua. Debe contar con la siguiente funcionalidad:

a) El visor de imágenes radiológicas debe ser completamente basado en tecnología HTML5 por lo que es Zero Footprint Viewer (ZFP) para cualquier tipo de usuario.
b) Debe permitir el acceso desde dentro (local) y fuera de la institución (remoto) a bases de datos de pacientes e imágenes.
c) A través del acceso local y remoto debe permitir revisar y efectuar post-procesamiento de imágenes de manera que la solución sea server side rendering y pueda gestionar grandes volúmenes de datos si problema, de acuerdo al nivel de privilegios del usuario.
d) Debe reconocer exámenes grabados en CD o DVD de otras Instituciones (formato DICOM) y permitir guardarlos dentro del Sistema. La visualización debe ser con intervención de usuario. “Para poder guardarlos en el PACS de la institución la data tiene que estar en formato DICOM”.
e) Debe proveer mecanismo que permitan gestionar de una manera eficiente las imágenes independientemente del tipo de usuario que interactúe con el sistema.
f) La imagen diagnóstica debe ser almacenada sin pérdidas de calidad, estándar DICOM, con el objetivo de realizar el diagnóstico radiológico actual o futura comparación al momento de realizar un diagnóstico.

g) La imagen de referencia debe ser liviana, contemplar el uso de compresión con pérdidas para referencia clínica, para distribución expedita de estas imágenes a los diferentes puntos de distribución.
h) Debe incluir actualizaciones provenientes de fábrica durante el período de contrato (garantía).
i) Debe permitir futuro crecimiento en modalidades y almacenamiento.
j) Debe permitir la visualización vía web en estaciones de visualización dentro y fuera del Departamento de Diagnóstico por Imágenes, las que deben contar con herramientas básicas de procesamiento de imágenes (zoom, pan, mediciones, etc.) considerando siempre imágenes con calidad diagnóstica.
k) La visualización vía web debe estar basada en sistemas operativos de cualquier tipo independiente también del navegador web y Sistemas de comunicación Estándar (DICOM, HL7, ASCII). Por lo que es necesario destacar que sería ideal una solución que no requiera descargar ningún plug-ins para visualizar la imagen bien sea para hacer diagnostico o no
l) La visualización concurrente de todas las imágenes debe ser en tiempo real, es decir, estar disponibles en forma inmediata para los usuarios, para diagnóstico y visualización clínica al mismo tiempo y de forma ilimitada.
m) La visualización de estudios debe ser multi browser (Microsoft Edge ó Chrome ó Mozilla ó Safari) y multi sistema operativo (Windows, Linux, OSX).
n) Debe tener un Sistema de análisis avanzado de imágenes 3D. Con funcionalidades para radiología y CT. Con funcionalidades de reconstrucción planar curva, endoscopía virtual, extracción de vasos, análisis de colon e hígado y perfusión cerebral.
o) Debe permitir grabación de estudios en CD o DVD en formato DICOM, con software auto ejecutable para la visualización de exámenes.
p) Deberá realizar la migración de la totalidad de estudios existentes en el sistema PACS actual del Hospital, a la solución PACS ofertada, de manera exitosa, el hospital brindará las facilidades del caso.
q) Debe permitir integración con solución impulsada por el MINSA para que todos los PACS de otros establecimientos de salud puedan acceder a las imágenes de acuerdo con el requerimiento de médico tratante del paciente.
r) Deberá proporcionar y facilitar toda la información necesaria para la migración de datos ante una posible renovación y/o actualización del RIS-PACS, en caso el HEJCU tenga la necesidad de implementar una nueva solución una vez terminado el tiempo de garantía. Las imágenes deberán estar en formato DICOM sin ningún tipo de compresión, encriptación, llaves u otros, para futuras migraciones que el hospital considere oportuno.
s) El PACS deberá contar con control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de privilegios asignados a los usuarios, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, u otro medio de identificación del usuario. Asimismo, deberá contar con una opción, reporte u otra herramienta, si fuera el caso, para que el área de informática pueda realizar una verificación periódica de los privilegios asignados, los cuales estarán definidos mediante un procedimiento documentado.
t) El PACS deberá generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.
u) El PACS deberá establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

v) El software PACS debe permitir la integración de estas herramientas con los Sistemas de Historia Clínica Electrónica, Telesalud y Servicios Médicos de apoyo en línea e interoperabilidad, de acuerdo a la implementación que viene realizando en los hospitales y su progresivo despliegue a nivel nacional en todos los establecimientos de salud del MINSA.

w) El Software PACS, se deberá contar con los accesos a las máquinas virtuales y base de datos de manera ilimitada sin restricción alguna, a fin de garantizar la continuidad de los servicios adquiridos en el futuro, al personal de informática del hospital.

x) El acceso y conexión al PACS por parte del proveedor, debe ser restringido y autorizado solo por los responsables informáticos del hospital en el momento que se requiera.

y) Se debe garantizar la licencia perpetua de todas las modalidades DICOM.

Manejo de datos del paciente

a) Debe tener comunicación sincrónica vía interfaz HL7, con la base de datos maestra de pacientes definida por la institución. El proveedor se encargará de la interconexión del servidor del RIS con los sistemas informáticos (HIS) que el hospital cuente al momento de la implementación, aun cuando estos no tengan HL7, además de que cada vez que el hospital ponga en funcionamiento un nuevo sistema informático que se relaciona con el departamento de imágenes, el proveedor deberá realizar la interconexión, sin costo adicional para el hospital mientras dure el contrato.

b) Debe manejar los siguientes datos: tipo de documento, número de identificación, número de identificación del paciente Historia Clínica (único para la institución), nombre completo, sexo, fecha de nacimiento, dirección, teléfono, tipo de financiador (SIS, SOAT, PARTICULAR), entre otros.

c) Debe permitir la actualización de los datos de los pacientes, cuando estos hayan sido actualizados o modificados en el módulo de admisión del HIS del hospital, sin la intervención de personal del departamento de diagnóstico por imágenes.

Consideraciones adicionales

a) Permite consolidar e integrar los estudios de diagnóstico por imágenes provenientes de múltiples equipos, incluso si estos equipos son de distintos fabricantes.

b) Permite realizar actualizaciones automáticas del software recurrente de cada estación de diagnóstico y de visualización.

c) La Interfaz Gráfica de Usuario (GUI) en las Estaciones de Diagnóstico debe guardar uniformidad (mismo esquema de colores y escala de grises) entre los monitores, con el fin de mantener el nivel de luminosidad de ellos, dentro de rangos aceptables para el diagnóstico.

d) La Interfaz Gráfica de Usuario (GUI) debe contar con barras de herramientas personalizables.

e) En el sistema las únicas imágenes válidas para diagnóstico son las imágenes DICOM, las imágenes en otros formatos pueden ser copiadas al informe radiológico, más no al estudio.

f) Permite la exportación automática de estudios a formatos gráficos estáticos: JPEG o TIFF y otros compatibles desde estaciones de trabajo y a PDF o HTML o XML, etc. desde PACS. También permite exportación a formatos de video: AVI o MPEG2 o QuickTime, etc. y correo electrónico.

g) Permite fijar preferencias para la visualización de imágenes según el tipo de equipo, tipo de examen o parte del cuerpo.

h) Las estaciones de diagnóstico radiológico deben incorporar herramientas de navegación multi-estudios que permita enlazar varias series de imágenes de distintos estudios para navegación comparativa.

i) El sistema RIS-PACS deberá poseer base de datos independientes sin necesidad de requerir integraciones de escritorio y consolidando toda la información para garantizar la integrabilidad de los datos. El sistema debe incluir la función “prefetching” de estudios anteriores, recuperando las imágenes históricas

residentes en el archivo de largo plazo al caché on line para todos los pacientes, de manera que permita contar con todos los estudios anteriores de forma instantánea al momento de realizar el diagnóstico.

j) El sistema debe permitir la visualización simultanea de estudios históricos en adelante de un mismo paciente para realizar comparaciones.
k) Permite a los recurrentes conectados al PACS contar con herramientas de búsqueda de estudios según cualquier criterio disponible (por ejemplo: nombre, DNI, fecha de examen, fecha de nacimiento, etc.).
l) El sistema debe incluir un mecanismo de "autolog off" para la desconexión automática de usuarios luego de haber transcurrido un periodo de tiempo determinado.
m) Como parte de la solución, es necesario ofrecer un sistema RIS y un sistema PACS de manera conjunta y totalmente integrada. La solución ofertada debe incluir sistemas PACS y RIS de la misma marca y fabricante que permitan una total integración entre estas aplicaciones.
n) La solución debe asegurar total independencia en la tecnología de almacenamiento empleada permitiendo la utilización de una amplia gama de opciones (SAN, NAS, CAS, etc.).
o) Con capacidad de reconocimiento de voz para el dictado de diagnóstico por imágenes.
p) Se requerirá licenciamiento del motor de base de datos.
q) El software PACS deberá contar con registro sanitario DIGEMID y/o certificado internacional de la FDA y/o EMA u otra institución internacional reconocida del modelo del sistema ofertado.
r) El software PACS deberá contar con ISO 13485:2003.
s) El software PACS deberá contar con estándares DICOM, CIFRADO SSL, HL7.

- **SUB-ITEM 1.2: SOFTWARE RIS**

  La solución debe contar con garantía de 05 años y licencia perpetua.

Generalidades

a) El sistema RIS ofertado debe ser flexible y altamente personalizable de manera que el cliente elija el flujo de trabajo que más se ajuste a sus necesidades.
b) Debe permitir incluir, modificar o eliminar formularios de datos de acuerdo al requerimiento del Departamento de Diagnostico de Imágenes del HEJCU.
c) Debe permitir integración con otros sistemas como HIS, LIS, Registros Clínicos Electrónicos, entre otros, mediante HL7, si alguno de los sistemas con los que cuenta el hospital al momento de la implementación no cuente con HL7, el proveedor deberá garantizar la conexión efectiva con estos sistemas de información mediante otros métodos. En caso de utilizar alguna herramienta de integración esta deberá ser asumida en su totalidad por el proveedor.
d) Debe permitir integrar nuevos módulos a implementar del sistema HIS que utiliza el hospital, esta deberá ser asumida en su totalidad por el proveedor.
e) Deberá permitir integración en caso que el hospital cambie de sistema HIS. Esta actividad deberá ser asumida en su totalidad por el proveedor.
f) Debe contar con la información del profesional responsable en cada etapa del proceso de atención y el tiempo de duración de cada una de éstas.
g) Debe permitir la firma digitalizada (escaneada) y firma electrónica de los profesionales que informan los exámenes y su impresión en los informes.
h) Debe permitir la definición de perfiles de usuario que determinen los derechos de acceso a diferentes niveles de la información de acuerdo con el rol que cumpla dentro o fuera del Departamento de Diagnóstico por Imágenes.

i) Debe contener la posibilidad de “pre-informe”, realizado por médico residente, para que luego pueda ser validado por medico radiólogo asistente, con la visualización e impresión final de los dos nombres responsables del informe.

j) Debe contar con base de datos, con la información de los médicos remitentes de las diferentes especialidades de la entidad, el hospital proveerá el listado de médicos y con la opción de poder actualizar a demanda por parte del área usuaria.

k) Debe utilizar el DNI y la Historia clínica como identificador de pacientes, sin perjuicio de poder incluir otros identificadores anexos.

l) Debe poder registrar los datos completos de cada examen y posibilidad de inserción de observaciones.

m) Debe permitir asignar codificación especial a cada examen correlacionado con el código definido por la Institución u otros códigos similares existentes manejados en el área, siendo obligatoria la codificación CPMS aprobado por el MINSA.

n) La herramienta de configuración debe permitir ajustar el RIS a las necesidades propias de servicios radiológico y parametrizar cada uno de los recursos y variables que permitan un óptimo funcionamiento.

o) El sistema debe gestionar nuevas cuentas de usuario y también modificar las ya existentes a medida que los procesos lo vayan requiriendo, todo ello sin necesidad de detener el flujo y sin costo adicional a la institución mientras dure la relación contractual con el hospital.

p) Debe permitir que cualquier estación de RIS sea punto de entrega de exámenes, sin perjuicio de que exista un punto de entrega centralizado.

q) El sistema RIS debe contar con un módulo que permita evaluar los tiempos de duración de cada proceso del flujo de trabajo y exportarlos en una planilla Excel, ya sea por prestación, por modalidad o por usuario en un período de tiempo.

r) Permite la gestión y control automatizado de pacientes, desde que se genera la orden de trabajo hasta que recibe informe/resultados.

s) Tendrá un módulo de reporte que pueda ser modificado y ajustado por el usuario sin intervención del fabricante

t) El sistema RIS debe permitir a los médicos poder informar desde fuera de la institución sin la necesidad de tomar una estación remotamente a través de un usuario / contraseña.

u) El sistema RIS deberá contar con control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de privilegios asignados a los usuarios, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, u otro medio de identificación del usuario. Asimismo, deberá contar con una opción, reporte u otra herramienta, si fuera el caso, para que el área de informática pueda realizar una verificación periódica de los privilegios asignados, los cuales estarán definidos mediante un procedimiento documentado.

v) El RIS deberá generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

w) El Sistemas RIS deberá establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

x) El software RIS debe permitir la integración de estas herramientas con los Sistemas de Historia Clínica Electrónica, Telesalud y Servicios Médicos de apoyo en línea e interoperabilidad, de acuerdo a la implementación que viene realizando en los hospitales y su progresivo despliegue a nivel nacional en todos los establecimientos de salud del MINSA.

y) Se deberá contar con los accesos a las máquinas virtuales y base de datos de manera ilimitada sin restricción alguna, a fin de garantizar la continuidad de los servicios adquiridos en el futuro, al personal de informática del hospital.
z) El acceso y conexión al RIS por parte del proveedor, debe ser restringido y autorizado solo por los responsables informáticos del hospital en el momento que se requiera.
aa) El sistema deberá traer integrado un tablero de control que permita hacer un seguimiento de las métricas de desempeño y carga de trabajo en vivo con un dashboard de fácil lectura y las métricas más relevantes del servicio.

Manejo de datos del paciente

a) Debe tener comunicación sincrónica vía interfaz HL7, con la base de datos maestra de pacientes definida por la institución. El proveedor se encargará de la interconexión del servidor del RIS con los sistemas informáticos HIS que el hospital cuente al momento de la implementación, esta integración debe ser bidireccional y en tiempo real, aun cuando estos no tengan HL7, además de que cada vez que el hospital ponga en funcionamiento un nuevo sistema informático que se relaciona con el departamento de imágenes, el proveedor deberá realizar la interconexión, sin costo adicional para el hospital mientras dure el contrato.
b) Debe manejar los siguientes datos: tipo de documento, número de identificación del paciente, Historia clinica (único para la institución), nombre completo, sexo, fecha de nacimiento, dirección, teléfono, tipo de financiador (SIS, SOAT, PARTICULAR), entre otros.
c) Debe permitir la actualización de los datos de los pacientes, cuando estos hayan sido actualizados o modificados en el módulo de admisión del HIS hospital, sin la intervención de personal del departamento de diagnóstico por imágenes.

Agenda y manejo del work flow

a) Debe contar con agenda que permita programar los exámenes en el departamento de Diagnóstico por Imágenes.
b) Debe proveer formularios (información y requisitos para el examen, comprobantes de citación, consentimiento informado, etc.), de manera automática, configurable e individualizada para cada paciente con orden.
c) Los formularios deben ser visibles en cualquier parte del flujo del RIS y desde cualquier modulo, que forme parte del RIS, si este es modular.
d) Debe permitir la configuración de agendas (Agenda multi recurso) y flujos para los recursos involucrados en la realización de exámenes (salas, equipamiento, médico), en un solo paso.
e) Debe proveer la solución más recomendable para la realización de un examen, con la combinación de disponibilidad y preferencias entre los distintos recursos involucrados en la realización del examen solicitado.
f) Debe permitir asignar al menos 3 niveles de prioridad para los exámenes, con posibilidad de marcar y/o destacar en las listas de trabajo de tecnólogos y radiólogos.
g) Debe permitir agendamientos combinados de estudios de distintas modalidades.
h) Debe permitir de manera simple el bloqueo de recursos (fallas, mantenimiento, vacaciones, etc.).
i) Debe permitir que las solicitudes médicas o solicitudes de examen, que vengan escritas en papel puedan ser escaneadas e incorporadas en los antecedentes del paciente.
j) Debe distribuir el trabajo según corresponda, a través de la función Worklist de las modalidades.
k) Debe generar diferentes listas de trabajo para cada una de las actividades del departamento de Diagnóstico por Imágenes, mediante la aplicación de distintos filtros de búsqueda, los que podrán ser

elaborados según el criterio de los usuarios. Estas listas deberán poder ser impresas o consultadas en la pantalla de cualquiera de las estaciones.

l) Debe dar soporte a la realización de los exámenes a través de la cadena de producción que se defina.
m) Debe llevar registro de los tiempos involucrados en cada etapa del proceso y de los usuarios que intervienen (recepción del paciente, inicio y fin del examen, generación de informe, entrega, etc.).
n) Cada etapa o dato, debe poder ser medido estadísticamente.
o) Debe soportar reconocimiento de voz para la realización de informes radiológicos.
p) Debe asegurar la asociación entre imagen e informe radiológico.
q) Debe permitir el registro de medicamentos e insumos utilizados en cada paciente.
r) Debe soportar la entrega de exámenes a pacientes, bajo los flujos de trabajo que defina el Departamento de Diagnóstico por Imágenes.
s) Cualquier estación RIS frente a una contingencia debe tener la capacidad de ser un punto de entrega de exámenes, sin perjuicio de que se haya centralizado en un solo punto la entrega de los mismos.

Visualización de exámenes a través de la web

a) El sistema debe ser full web, incluyendo todos los módulos de RIS, PACS y Reconocimiento de Voz.
b) Debe permitir la consulta de exámenes e imágenes utilizando equipos (PC) existentes y nuevos en el Hospital, independiente del navegador y el sistema operativo. Es preciso mencionar que la red LAN del HEJCU y Red LAN del RIS/PACS deberán interconectarse sin ningún problema.
c) Debe mostrar imágenes representativas (JPG o similar compatible)
d) Debe permitir visualización múltiple de varios estudios simultáneos del mismo o varios pacientes.
e) Debe permitir la comparación con exámenes previos del paciente de manera rápida y oportuna. Para esto es necesario que el sistema tenga la opción de configurar un prefetching según los parámetros que defina el centro (modalidad, especialidad, parte del cuerpo, fecha, etc.).
f) La visualización vía WEB debe poseer herramientas básicas de manejo de imágenes como modo comparación con estudios previos, de fácil configuración, zoom y desplazamiento de la imagen, control del brillo y contraste, rotación de imagen, anotaciones, entre otras.
g) Incluye licencias ilimitadas para visualización.
h) El visualizador debe ser multinavegador y multisistema operativo
i) El sistema debe permitir la entrega de informes e imágenes mediante la página web de la institución desde cualquier sistema operativo, sea de un computador o un móvil; el cual será implementado en un servidor virtual a parte por temas de seguridad.

Especificación de reportes.

a) Debe disponer de reportes flexibles que pueda indicar, por rango de fechas, las consultas efectuadas, la identificación del usuario, la fecha; hora y terminal de origen de la consulta.
b) Debe especificar reportes de pacientes por tipos de examen y/o por datos demográficos.
c) Debe tener la capacidad de exportar reportes en formato Excel y/o Word y/o power point, sin prejuicio de poder tener un formato de reporte establecido.
d) Debe usar como identificador del paciente el número de la Historia Clínica y numero de documento de identidad.
e) El sistema debe cargar exámenes e imágenes anteriores del historial del paciente en adelante, previamente al diagnóstico.
f) Debe permitir administración del Flujo de Trabajo, permitiendo la distribución y direccionamiento de imágenes e informes a los distintos niveles de usuarios.
g) Permite generación y gestión de informes de texto enriquecido, .doc e informes estructurados DICOM (SR) estándar.

Software para control de gestión

a) Incluye herramientas de software para la elaboración de informes de gestión.
b) Debe proveer funcionalidades destinadas a controlar la gestión, mediante la emisión de reportes preestablecidos.
c) El sistema debe generar reportes que indiquen como mínimo: estadísticas de producción; producción por tipo de examen; productividad por modalidad, por tipo de profesional, consumo de insumos (en cantidades) y otros reportes que requeridos por el Departamento de Diagnóstico por Imágenes.
d) Estos reportes deben ser detallados por centro de producción y sus respectivos servicios de atenciones de emergencia y hospitalización del HEJCU.
e) Número de códigos de prestación informados por cada médico, en un periodo dado, separados por modalidad.
f) Prestaciones sin informe (no informadas). La unidad de medida deberá parametrizarse en conjunto con el Hospital.
g) Debe incluir la Procedencia de los pacientes.
h) El sistema debe integrar el código de Seguro de Salud y otros códigos similares que se manejan a nivel del sector público o privado.
i) El sistema deberá proveer reporte estadístico de producción de exámenes según código CPMS por modalidad, por personal, por origen de solicitud (servicio).

Diagnóstico remoto

a) Debe permitir que exámenes sean informados, remotamente vía web, sin restricción de funcionalidades, por médicos radiólogos que se encuentren ubicados fuera de la institución. En particular, el reconocimiento de voz debe poder ser utilizado remotamente con la misma calidad de reconocimiento que en el Hospital.

Almacenamiento de imágenes

a) Debe almacenar imágenes en formato DICOM, sin pérdida, para todo el volumen de exámenes de este contrato.
b) Debe permitir disponer de los exámenes realizados en forma ilimitada online, de manera tal, que tanto radiólogos y clínicos tengan acceso inmediato a través de las herramientas de software definidas para cada uno.
c) Debe ser escalable, con el fin de ampliar la capacidad de almacenamiento ilimitadamente en caso de un crecimiento mayor al esperado en la Unidad.

Licencias

a) Se requerirá licenciamiento RIS ilimitado en todos los módulos solicitados y perfiles, asegurando que la eliminación o solicitud de licencias extras no tienen costo alguno para la institución.
b) Se requerirá licenciamiento PACS ilimitado y perpetuo en todos módulos solicitados y perfiles, asegurando que la eliminación o solicitud de licencias extras no tienen costo alguno para la institución. La producción de estudios anual a ser cubierta es de 150,000 estudios como mínimo.
c) Se requerirá licenciamiento de reconocimiento de voz, asegurando que la eliminación o solicitud de licencias extras no tienen costo alguno para la institución para 25 usuarios concurrentes, con ilimitados usuarios intercambiables.
d) Se requerirá licenciamiento de Software de Visualización, Diagnóstica y Clínica ilimitado en todos sus perfiles, asegurando que la eliminación o solicitud de licencias extras no tienen costo alguno para la institución.
e) Se requerirá licenciamiento del motor de base de datos.

f) El software ofrecido de RIS, PACS, visualizadores, reconocimiento de voz y/u otro que se oferte, debe ser licenciado, de carácter propietario o privativo, de código cerrado, para lo cual, la empresa que desarrolle el software debe tener los derechos de autor de la totalidad del software y debe presentar los certificados correspondientes por cada módulo señalado anteriormente. No se aceptarán ofertas en que los componentes modulares de la solución sean de origen de software libre, GNU u Open Source.
g) Se debe garantizar la licencia perpetua de todas las modalidades DICOM.

Consideraciones Adicionales

a) La información del sistema RIS deberá disponer de un catálogo ("árbol") de los distintos exámenes que pueden ser requeridos desde cualquier estación de diagnóstico o visualización.
b) El sistema RIS debe permitir "forzar citas", según el nivel de permisos del usuario, con el fin de atender a los pacientes en un mismo periodo de tiempo.
c) El sistema debe asegurar una integración de escritorio ("desktop integration") a nivel de estación de diagnóstico y de visualización, de modo que las pantallas RIS y PACS de las estaciones se manejen con único teclado y mouse.
d) La plataforma de integración HL7 con la historia clínica electrónica deberá incorporar interfaces ORM para la recepción de órdenes y solicitudes y el envío de confirmaciones.
e) Al momento de generar una orden de examen, el sistema deberá tener la capacidad de imprimir documentos que señalen la preparación requerida para cada examen, pudiéndose configurar y asociar estos documentos a un examen en particular o a un grupo de exámenes.
f) El módulo de programación de orden de exámenes del RIS debe ser independiente del módulo de datos clínicos del paciente con el fin de garantizar la confidencialidad de la información.
g) El sistema debe incluir herramientas de ayuda y manuales de usuario en línea.
h) El sistema debe permitir el registro del o los exámenes solicitados a un paciente y configurar el equipo en el cual se realizarán de acuerdo con los parámetros del examen.
i) El sistema deberá proveer el servicio de lista de trabajo a los equipos de adquisición de imágenes conectados que dispongan de licencia DICOM Modality WorkList.
j) El (los) Servidor(es) RIS son independientes del (los) servidor(es) del sistema PACS.

- **SUB-ITEM 1.3: SOFTWARE DE RECONOCIMIENTO DE VOZ**

La solución debe contar con garantía de 05 años y debe ser licencia perpetua. Debe contar con la siguiente funcionalidad:

a) Software de reconocimiento de voz para 25 usuarios concurrentes como mínimo.
b) Interfaz intuitiva.
c) Compatible con cualquier editor de texto.
d) Entrenamiento sencillo.
e) Diccionario específico para radiología, con acrónimos, siglas, abreviaturas.
f) Debe permitir agregar términos, cambiar términos, modificar su pronunciación.
g) Aprendizaje continuo de nuevas palabras que utiliza cada usuario.

3.2.2 ITEM 2: DICTAFONOS

a) Cantidad: 06
b) Micrófono desacoplado independiente.
c) Filtro integrado.
d) Sensor de movimiento con respecto al micrófono, cuando se está en modo grabación, y al ponerlo en su pedestal y/o base, la grabación se pone en modo pausa, y luego se activa la grabación al retirarlo, para continuar la grabación.

e) Carcasa y botones ergonómicos.
f) Rueda de desplazamiento para función de mouse integrada.
g) Conectividad mediante puerto USB 2.0 de alta velocidad.
h) Cable de 2.5mt.
i) Altavoz dinámico incorporado.
j) Soporte para micrófono.
k) Manual de usuario.
l) Debe contener comandos de voz, para interactuar con la aplicación y el texto.

3.2.3 ITEM 3: TERMINALES VDI - ESTACIONES DE VISUALIZACIÓN

CARACTERÍSTICAS	DESCRIPCIÓN
Cantidad	40
Procesador	APU SoC Dual-Core con soporte gráficos (frecuencia base de 1,5 GHz, frecuencia de ráfaga de hasta 2 GHz, 1 MB de caché)
Flash/RAM	Hasta 512GB flash/hasta 16 GB SDRAM DDR4 - 186620
Resolución máxima	3840 x 2160 vía DisplayPort™
Pantallas admitidas	2 x DisplayPort™
Interfaz de red integrada	LAN: Gigabit Ethernet (RJ-45) WLAN: Doble Banda (2,4 GHz y 5 GHz)
Serie	1
Paralelo	Opcional
USB	3 USB-A 3.1 2 USB-A 2.0 1 USB 3.1 Type-C™
Ranura de bloqueo por cable	Sí
ENERGY STAR®	Sí
EPEAT®	Sí
Bajo contenido en halógenos	Sí
Periféricos incluidos	Mouse: Cada terminal debe incluir un mouse con las siguientes características: • Interface USB. • Óptico. • 2 botones con SCROLL. • Ser del mismo fabricante del terminal VDI. Teclado: Cada terminal debe incluir un teclado con las siguientes características: • Interface USB, en idioma español • Ser del mismo fabricante del terminal VDI.
Accesorios	El enchufe del cable de alimentación eléctrica debe ser para toma Schuko Tipo L.
Monitor	Cada estación VDI debe incluir un monitor LED con las siguientes características: • Tamaño: 22” o superior. • Resolución: 1920 x 1080, 60 Hz o superior.

	• Resolución de aspecto: 16:9. • Brillo: 250 cd/m2 o superior. • Relación de contraste: 1000:1 o superior. • Puertos: 01 DisplayPort o superior. • Fuente de alimentación: Voltaje de entrada: 100 a 240 VCA o superior • Accesorios: o Cable DisplayPort o El enchufe del cable de alimentación eléctrica debe ser para toma Schuko Tipo L.
LICENCIA	Windows Pro 11 o superior
GARANTÍA	La garantía de fábrica y soporte a través de CAS autorizado de la marca debe ser por un periodo de cinco (05) años o superior.

El proveedor debe incluir en su propuesta los racks para las estaciones VDI (Monitor, CPU, Teclado y Mouse de acuerdo a los equipos ofertados).

3.2.4 ITEM 4: TERMINALES VDI - ESTACIONES DE DIAGNOSTICO

CARACTERÍSTICAS	DESCRIPCIÓN
Cantidad	4
Procesador	APU SoC AMD Dual-Core con gráficos (frecuencia base de 1,5 GHz, frecuencia de ráfaga de hasta 2 GHz, 1 MB de caché)
Flash/RAM	Hasta 512GB flash/hasta 16 GB SDRAM DDR4 - 186620
Pantallas admitidas	3 x DisplayPort™
Interfaz de red integrada	LAN: Gigabit Ethernet (RJ-45) WLAN: Doble Banda (2,4 GHz y 5 GHz)
Serie	1
Paralelo	Opcional
USB	3 USB-A 3.1 2 USB-A 2.0 1 USB 3.1 Type-C™
Ranura de bloqueo por cable	Sí
ENERGY STAR®	Sí
EPEAT®	Sí
Bajo contenido en halógenos	Sí
Periféricos incluidos	Mouse: Cada terminal debe incluir un mouse con las siguientes características: • Interface USB. • Óptico.

	• 2 botones con SCROLL. • Ser del mismo fabricante del terminal VDI. Teclado: Cada terminal debe incluir un teclado con las siguientes características: • Interface USB, en idioma español • Ser del mismo fabricante del terminal VDI. UPS: Cada terminal debe incluir un UPS de 1.5 KVA o superior, Monofásico 220VAC,60HZ, Tipo rack/torre con autonomía de 10 minutos o superior. Considerar: • Instalación: El servicio de instalación y puesta en marcha deberá ser realizado por especialistas debidamente preparados para la instalación. • Accesorios: El proveedor deberá considerar todos los accesorios necesarios para el funcionamiento del UPS, deberá incluir cables de poder necesarios para los equipos conectados al UPS. El enchufe del cable de alimentación eléctrica del UPS deberá ser Schuko Tipo L. Scanner: Cada terminal debe incluir un Scanner de tamaño compacto. Considerar: • Capacidad de alimentador automático de documentos (ADF): 20 hojas como minimo. • Resolución Óptica: 600dpi • Tamaño hojas escaneo: A4, A5, Legal, Oficio. • Volumen diarias: 1000 páginas o superior • Opciones de escaneo: doble cara con una sola pasada. • Formato de archivos escaneados: PDF, PDF con capacidad de búsqueda, JPG, BMP, Microsoft Excel, Microsoft Word. • Conectividad: USB 3.2 o superior. • Velocidad de escaneo: Hasta 30ppm o superior • Tamaño de papel admitido: A4, A5, A6, Oficio, Legal. • Normas medioambientales: ENERGY STAR. • Fuente de Alimentación: 100 V – 240 V. • Software: Herramientas para edición de escaneo. • Funcionalidad: Detección automática de color, recorte automático, corrección de inclinación automática, rotación automática, detección de página en blanco, ajuste de brillo y contraste, compresión JPEG, combinación de imágenes, entre otros. • Accesorios: Cable de poder y adaptador Schuko Tipo L certificado • Sistema Operativo Compatible: Windows 10, Windows 11.
Accesorios	Cable de poder y adaptador | Schuko Tipo L certificado

Monitor de Grado Medico	Cada estación VDI debe incluir dos monitores con las siguientes características: • Tipo: IPS 21" Color ó superior • Pixeles: 2 Megapíxeles como mínimo y de grado médico. • Luz de fondo LED. • Resolución: 1600 x 1200 o superior. • Luminosidad: 500 cd/m2 o superior. • Relación de contraste: 1400:1 o superior. • Puertos: DisplayPort. • Fuente de alimentación: Voltaje de entrada: 100 a 240 VCA o superior • Rotación: 90° (pivote). • Certificación: FDA, CE. • Accesorios: o Cable DisplayPort o Cable de poder y adaptador Schuko Tipo L certificado.
Monitor	Cada estación VDI debe incluir un monitor LED con las siguientes características: • Tamaño: 22" o superior. • Resolución: 1920 x 1080, 60 Hz o superior. • Resolución de aspecto: 16:9. • Brillo: 250 cd/m2 o superior. • Relación de contraste: 1000:1 o superior. • Puertos: 01 DisplayPort o superior. • Fuente de alimentación: Voltaje de entrada: 100 a 240 VCA o superior • Accesorios: o Cable DisplayPort o Cable de poder y adaptador Schuko Tipo L certificado.
Licencia	Windows Pro 11 o superior Suite de Ofimática vigente
Garantía	La garantía de fábrica y soporte a través de CAS autorizado de la marca debe ser por un periodo de cinco (05) años o superior.

Ubicación de las Estaciones de Visualización:

SEDE CENTRAL HEJCU		
PISO	**LOCALIZACIÓN**	**ESTACIONES DE VISUALIZACION**
1	CONSULTORIO DE URGENCIAS	2
	UCI 2	1
	TRAUMA SHOCK 2	1
	PEDIATRÍA	1
	TRAUMA SHOCK	2

SEDE CENTRAL HEJCU		
PISO	**LOCALIZACIÓN**	**ESTACIONES DE VISUALIZACION**
	CARDIOLOGIA	1
	TOPICO 1	1
	TÓPICO 2	1
	MEDICINA FISICA Y REHABILITACIÓN	1
	GINECOLOGIA	1
	TRAUMATOLOGÍA	3
	TOMOGRAFIA	2
	ECOGRAFIA	3
2	STAR SALA DE OBSERVACION	1
	HOSPITALIZACION DE NEUROCIRUGIA	1
	GASTROENTEROLOGIA	1
	OFICINA DE DIRECCIÓN GENERAL	1
	COORDINACIÓN MÉDICA	1
	JEFATURA DE DIAGNOSTICO POR IMÁGENES	1
3	UCI	1
	UCIN	1
	NEUROCIRUGIA	1
	SALA DE OPERACIONES 1	1
	SALA DE OPERACIONES 2	1
	SALA DE OPERACIONES 4	1
	SALA DE RECUPERACIÓN	1
	ESTACION DE ENFERMERAS	1
	STAR HOSPITALIZACION DE TRAUMATOLOGÍA	1
4	STAR HOSPITALIZACION DE CIRUGIA	1
	JEFATURA DE CIRUGÍA	1
5	STAR HOSPITALIZACION DE MEDICINA	1
	JEFATURA DE MEDICINA	1
6	OFICINA DE ESTADÍSTICA E INFORMATICA	1
TOTALES		**40**

3.2.5 ITEM 5: PANTALLAS DE VISUALIZACION PARA SALA DE OPERACIONES

DESCRIPCIÓN	CARACTERÍSTICAS
CANTIDAD	• 3
PANTALLA	• Tamaño 55” o superior. • Ultra HD 4K / SMART TV. • Tecnología Mini LED. • Curvo: NO.

DESCRIPCIÓN	CARACTERÍSTICAS
	• Resolución 3840 x 2160 (4K). • Tasa de Refresco de 120 Hz. • Antirreflejo.
VIDEO	• Procesador Inteligente de Imágenes 4K. • HDR10, HLG, HDR 10+ y/o Dobly Vision IQ.
CONECTIVIDAD	• 02 HDMI o superior. • 01 Puerto Ethernet (LAN) • 02 Puerto USB o superior. • Wi-fi 5 (802.11ac) o superior • Bluetooth v5.x o superior.
SONIDO	• Dolby Atmos.
FUENTE DE ALIMENTACIÓN	• AC 100 – 240 V 50-60 Hz.
AÑO DE FABRICACIÓN	• 01 año de antigüedad.
RACK	• Incluye Rack Giratorio para TV. • El Rack tiene que ser acondicionado para ser empotrados en la pared.
ACCESORIOS	• Incluir cable HDMI 4K de 10 metros. • Incluir adaptador de DisplayPort a HDMI. • Cable de poder y Adaptador Schuko Tipo L certificado.
GARANTÍA	• La garantía de fábrica y soporte a través de CAS autorizado de la marca debe ser por un periodo de cinco (05) años o superior.

3.2.6 ITEM 6: TECLADO MEDICO PARA SALA DE OPERACIONES

DESCRIPCIÓN	CARACTERÍSTICAS
CANTIDAD	3
TECLADO	• Lavable, Impermeable, Antibacteriano y/o de Silicona.
	• Preferencia en Idioma Español.
	• Protección NEMA 4X y IP68 o Superior.
COMPATIBILIDAD	• Compatible con todas las Versiones de Windows existentes actualmente.
CONECTOR	• USB
GARANTÍA	• Garantía debe ser por un periodo de cinco (05) años o superior.

3.2.7 ITEM 7: MOUSE MEDICO PARA SALA DE OPERACIONES

DESCRIPCIÓN	CARACTERÍSTICAS
CANTIDAD	3
MOUSE	• Lavable, Impermeable, Antibacteriano y/o de Silicona.
	• Protección NEMA 4X y IP68 o Superior.
COMPATIBILIDAD	• Compatible con todas las Versiones de Windows existentes actualmente.
CONECTOR	• USB superior.

3.3 COMPONENTE EQUIPOS BIOMEDICOS:

Este componente se encuentra conformado por los ítems:

ITEM	DESCRIPCIÓN	CANTIDAD
1	Digitalizador	1
2	Chasis de Fosforo	12
3	Impresora láser de películas radiográficas	1

3.3.1 ITEM 1: DIGITALIZADOR

Debe contar con las siguientes características:

a) Digitalizador CR de chasis múltiple.
b) Resolución de escala de grises en adquisición de datos de 12 bits/píxel como mínimo.
c) Capacidad para procesar 90 o más placas por hora en formato 14" x 17".
d) Incluye estación de procesamiento de imágenes.
e) Incluye monitor LCD de pantalla táctil de 17" o más.
f) Incluye software avanzado para el procesamiento de imágenes, garantizando altos estándares diagnósticos, con interfaz de usuario a través de pantalla táctil.
g) El software permite hacer marcas, anotaciones, rotar la imagen, hacer magnificaciones (zoom), mediciones de distancias y ángulos, variar window/level, colimación, impresión de varias imágenes en una sola placa, suprimir líneas de grilla.
h) El digitalizador utiliza chasises con memoria incorporada para almacenar los datos del paciente sometido a examen y lectora de código de barras del chasis.
i) Capacidad para seleccionar los datos del paciente directamente desde una lista de trabajo RIS/HIS.
j) Incluye módulo para exportar imágenes DICOM a CD ROM. autoejecutable en cualquier Pc.
k) Permite enviar las imágenes digitalizadas a un Archivo Digital de Imágenes Diagnósticas (PACS) o a un Sistema de Impresión Láser.
l) Cumple estándares DICOM (DICOM Print, DICOM Storage, DICOM modality Work list, DICOM Send)
m) Cumple estándares IHE.
n) Cumple normas de seguridad UL, CE.
o) Cumple estándares HIPAA.
p) Alimentación eléctrica de 220v.

3.3.2 ITEM 2: CHASIS DE FOSFORO:

- **SUB-ITEM 2.1: CHASIS DE FOSFORO - TAMAÑO 43 X 35CM**

(CANTIDAD: 06)

Las pantallas de fósforo de GP (propósito general), como son consumibles, deben garantizar como mínimo 40 000 exposiciones (de ser menor la capacidad de las pantallas se deberá garantizar con cumplir el número de exposiciones solicitadas). Estas estarán debidamente acreditadas por el fabricante o representante.

- **SUB-ITEM 2.2 CHASIS DE FOSFORO - TAMAÑO 18 X 24CM**

(CANTIDAD: 06)

Las pantallas de fósforo de GP (propósito general), como son consumibles, deben garantizar como mínimo 40 000 exposiciones (de ser menor la capacidad de las pantallas se deberá garantizar con cumplir el número de exposiciones solicitadas). Estas estarán debidamente acreditadas por el fabricante o representante

3.3.3 IMPRESORA LASER DE PELICULAS

a) Impresora Láser de películas, con tecnología láser, de última generación.
b) Mínimo de tres formatos on line.
c) Tamaño del píxel igual o menor a 50 micrones.
d) Mayor o igual a 508 dpi de resolución, con capacidad de impresión con píxeles de borde definido.
e) Capacidad para procesar como mínimo 75 placas/hora en 14" x 17".
f) Capaz de imprimir en formatos 8" x 10", 11" x 14" o 10 x 14 y 14" x 17".
g) Incluye como mínimo tres bandejas de películas que permitan imprimir en tres formatos de película en simultáneo, a elección. (p.e. 8" x 10", 11" x 14" ó 10 x 14 y 14" x 17").

Hospital de Emergencias Jose Casimiro Ulloa

Firmado digitalmente por ALLPAS GOMEZ Henry Lowell FAU 20138100015 soft
Motivo: Soy el autor del documento
Fecha: 06.02.2025 17:58:29 -05:00

Hospital de Emergencias Jose Casimiro Ulloa

Firmado digitalmente por SILVA BUITRON Giancarlos FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:05:43 -05:00

Hospital de Emergencias Jose Casimiro Ulloa

Firmado digitalmente por PACHAS SUAREZ Carlos Abraham FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:01:32 -05:00

Hospital de Emergencias Jose Casimiro Ulloa

Firmado digitalmente por OCHOA DELGADO Isabel Milagros FAU 20138100015 hard
Motivo: Doy V° B°
Fecha: 06.02.2025 17:11:12 -05:00