PROGRAMA MEJORAMIENTO DE LOS SERVICIOS DE JUSTICIA EN MATERIA PENAL EN EL PERÚ — PMSJMPP

Contrato de Préstamo N° 4959/OC-PE

ESPECIFICACIONES TECNICAS

Adquisición de una "Solución: de Servidores y Storage, de Ampliación de Capacidad de Almacenamiento y de Respaldo de la Solución de Servidores y Storage"

I. Antecedentes

La República del Perú y el Banco Interamericano de Desarrollo (BID), suscribieron el Contrato de Préstamo N° 4959/OC-PE, con el objeto de contribuir al financiamiento y ejecución del Programa de Inversión: "Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú - CUI 2413075", en adelante el Programa. El financiamiento por parte del BID se encuentra sujeto a las disposiciones estipuladas en dicho Contrato de Préstamo y el Manual de Operaciones del Programa.

El objetivo general del Programa es la mejora de la gestión del servicio del Sistema de Administración de Justicia Penal (SAJP), a través de tres componentes: (1) aumento de la eficiencia del SAJP a través de medios tecnológicos; (2) aumento de la calidad de la investigación criminal; y (3) mejoramiento del acceso a los servicios de administración de justicia penal a través de medios tecnológicos.

Las entidades beneficiarias del Programa son el Poder Judicial (PJ), el Ministerio Público (MP) y el Ministerio de Justicia y Derechos Humanos (MINJUSDH), quienes, a su vez actúan como organismos ejecutores cada uno con una Unidad Ejecutora. Para el caso del MINJUSDH, el organismo ejecutor es la Unidad Ejecutora denominada "Unidad Ejecutora 005: Programa Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú — PMSJMPP".

La Unidad Ejecutora "Programa Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú", en adelante UE – PMSJMPP, tiene a su cargo la ejecución del componente 3 del Programa. Este componente, comprende la ejecución del proyecto de inversión "Mejoramiento de los servicios de información del MINJUSDH para la implementación de la interoperabilidad en materia penal - CUI 2412557", (en adelante Proyecto) el cual contribuirá a mejorar los servicios prestados a ciudadanos, funcionarios del Sistema de Administración de Justicia Penal (SAJP) y jóvenes en conflicto con la ley, a través de la disponibilidad de información pública, bajo un enfoque de datos abiertos.

La infraestructura tecnológica del MINJUSDH debe encontrarse adecuadamente operativa con el fin contar con una plataforma base para que sus sistemas puedan operar en condiciones adecuadas mínimas, superando su estado crítico actual.

En ese sentido, dada su importancia como plataforma base de los sistemas de información se ha realizado un análisis técnico a la plataforma tecnológica del MINJUSDH a cargo de su Unidad de "Supervisión de Infraestructura Tecnológica" y en compañía del técnico designado por la unidad beneficiaria, con el propósito de contar con estándares mínimos de operación de manera que garanticen la implementación de la interoperabilidad en materia penal.

II. Objetivo

Dotar de condiciones adecuadas, a nivel de infraestructura tecnológica (Servidores y Storage) al Centro de Datos de la sede central y sede alterna del MINJUSDH, los cuales brindarán el soporte tecnológico necesario para el funcionamiento de los sistemas de información del MINJUSDH: Solución Tecnológica para la Gestión de la Carpeta Defensorial y el Expediente de Extradiciones y Traslados.

III. Finalidad Pública

Garantizar la confianza de los usuarios internos (servidores de la entidad) y externos (ciudadanos) en el uso de los servicios digitales prestados por el **MINJUSDH** en cumplimiento del Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital en las entidades públicas[1].

IV. Área Solicitante

MINJUSDH

V. Alcance y Características del Bien

- **Alcance**

  Realizar el análisis técnico de lo propuesto en el perfil del proyecto con respecto a la infraestructura de equipos tecnológicos para la *"***Solución: de Servidores y Storage, de Ampliación de Capacidad de Almacenamiento y de Respaldo de la Solución de Servidores y Storage"** y las necesidades que actualmente presenta el **MINJUSDH**. Además, de brindar una solución técnica a nivel de la infraestructura de Equipos Tecnológicos (servidores y Storage).

La Adquisición de *"***Solución: de Servidores y Storage, de Ampliación de Capacidad de Almacenamiento y de Respaldo de la Solución de Servidores y Storage",** comprende la sede central del MINJUSDH, en la dirección que se detalla:

1. Sede Central – **MINJUSDH (Calle Scipion Llona 350, Miraflores, Lima)**

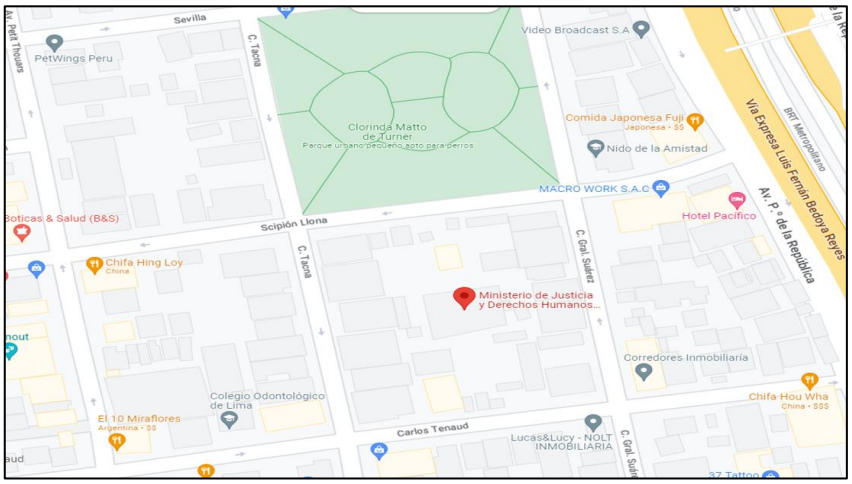

Imagen 1 Ubicación sede central MINJUS

[1] Numeral 9.1, que dispone que las entidades de la administración pública deben "c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información".

Los bienes serán entregados e instalados, según detalle:

Caso 1:
Ítem 1 "**Solución de Servidores y Storage**" e ítem 3 "**Solución de Respaldo de la Solución de Servidores y Storage**"; en un plazo máximo de ciento veinte (120) días, a Suma Alzada (a todo costo).

Caso 2:
Ítem 2 "**Solución de Ampliación de Capacidad de Almacenamiento**"; en un plazo máximo de ciento ochenta (180) días, a Suma Alzada (a todo costo).

- Los Contratistas / Proveedores interesados, deberán presentar oferta por cada ítem; asimismo, están obligadas a presentar oferta por los tres (3) ítems, indicando el monto total propuesto.

- Un solo Contratista / Proveedor será seleccionado para la adjudicación de contrato de todos los ítems.

➢ **Características mínimas del Bien**

Ítem 1: Equipamiento Sede Central - Solución de Servidores y Storage

A) CHASIS BLADE	
Cantidad de Chasis	Uno (01)
Factor de Forma	Máximo 10U debe incluir rieles para montaje en Rack
Módulo de administración	Dos módulos en redundancia y reemplazables en caliente
Interfaces I/O	Debe soportar la interconexión: Ethernet 10/25/100 Gb y Fibra Canal 16/32 Gbps.
	Debe contar con siete bahías como mínimo para equipos de interconexión.
	El sistema deberá soportar redes virtuales por puerto físico del módulo de cómputo y permitir administrar las direcciones físicas (MAC Address y WWN correspondientes) del mismo asignado a cada red virtual.
	Los puertos de todos los switches o módulos LAN/SAN que forman parte de la solución de Modulo de Cómputos, deberán estar licenciados en su totalidad.
	Los switches o módulos LAN/SAN deberán incluir las licencias de todas sus funcionalidades para todos sus puertos para futuros crecimientos
Conectividad LAN/SAN Convergente FC	Al menos dos (2) switches o módulos de conectividad convergente IEEE DCB Ethernet dentro del chasis con soporte de 10/25/40/100GbE para LAN y FC 16/32Gbps para SAN, instalados de manera redundante y en alta disponibilidad, minimo con 8 puertos cada uno.
	Con los switches o módulos ofertados, se debe ofertar entre un ancho de banda de "downlink" de conexión Ethernet de 50Gbps distribuido en forma redundante (dos o más puertos) hacia cada uno de los servidores en el Chasis.
	Se deberá habilitar al menos cuatro (04) conexiones o puertos uplink de 25GbE en cada switch o módulo LAN (cuatro conexiones total externos) para la conexión hacia los switches del MINJUS

A) CHASIS BLADE	
	Se deberá habilitar al menos cuatro (04) conexiones o puertos uplink FC nativo de 32Gbps en cada switch o módulo para la conexión SAN
	Rendimiento no menor a 6Tbps full duplex
	Latencia no mayor a 1µs
	Soporte de protocolos de Capa 2 (802.1D, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1t) Capa 3 (BGP, OSPF)
	Conectividad con soporte de IPv4 e IPv6
	Se deberá incluir los accesorios necesarios para la interconexión con los switches y otros equipos como los Transceiver y cables
Configuraciones & Funcionalidades mínimas requeridas	El Chasis debe ser de última generación lanzada por el fabricante con la finalidad de soportar actualizaciones de nueva generación.
	Capacidad slots soportados de al menos la cantidad de servidores del tipo 1 solicitados. Se podrán apilar chasises manteniendo una arquitectura de conectividad integrada para soportar los servidores requeridos en caso sea necesario para un futuro crecimiento.
	El Chasis debe soportar servidores de 2 procesadores como mínimo
	Debe soportar equipos de interconexión (módulos o switches) LAN de 10/25/40/100 GbE, con soporte de arquitecturas convergentes (FCoE), así como switches FC 16/32Gbps
	El chasis podrá ser libre de la dependencia de backplane/midplane o en caso se provean chasises con backplane/midplane, deberán ser de al menos 10Tbps.
Fuentes de poder y ventiladores	Incluye los PDUs necesarios (de acuerdo con la recomendación del fabricante) para soportar la máxima carga soportada por el chasis.
	Fuentes de 100-240 V AC @ 50/60 Hz, de clase Platinum.
	Las fuentes de poder y los ventiladores deben ser redundantes y hot-swap.
	Las fuentes de poder deben estar integrados en el Chasis y deberán permitir ser configuradas N+N con cualquiera de los procesadores soportados en su máxima configuración.
	La configuración de los ventiladores de estar en redundantes N+1 o superior y configuraciones para el correcto enfriamiento del chasis trabajando a carga completa.
Administración y Monitoreo	Consola de administración desde un portal web centralizado, con un software de gestión totalmente licenciado de manera perpetua, e implementado como un dispositivo *(appliance)* virtual, que permita administrar y gestionar de manera remota el funcionamiento de todos los componentes internos del chasis, incluyendo servidores y dispositivos de E/S, etc., a través de “dashboard” o tablero general.
	Debe de poseer integración nativa a través de APIs estándares tipo RESTful.
	Auto-descubrimiento y Monitoreo de todos los componentes (chasis, servidores, dispositivos de E/S), con notificaciones por correo electrónico.
	Debe tener una funcionalidad KVM virtual en tiempo real.
	Soporte de soluciones tipo contenedores (containers) y gestión de la solución como un pool de recursos gestionados a través del código de la aplicación.
	Soporte de acceso remoto para encendido y apagado de servidores, así como procesos de instalación y actualización remota de manera segura, con la funcionalidad de bloqueo del servidor en caso de un

A) CHASIS BLADE	
	intento de modificación de configuración o firmware no autorizado o malicioso.
	La solución debe tener la capacidad de diseñar perfiles y plantillas de perfiles de los servidores de cómputo, los cuales permitan configurar el BIOS, actualizar Firmware y Drivers, arreglos de los discos internos.
Gestión Automatizada	Debe contar con una plataforma de acceso y transmisión de data segura de monitoreo proactivo y 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.
	Debe permitir una vista consolidada de todos los servidores, permitiendo acceder a visualizar el estado de los componentes, estado de garantía, visualización de rendimiento (CPU, memoria, IOPS, consumo de energía y situación térmica).
	Debe permitir el envío de notificaciones sobre el estado de los componentes (uno o múltiples), así como el acceso a recomendaciones en caso requerirlas.
	Debe proveer supervisión de riesgos, con la capacidad de detección de anomalías de rendimiento que incluyan: * Visualización del rendimiento de CPU, memoria, IOP, térmica y energía. * Puntuaciones del estado del servidor, detalles y notificaciones de suscripción, para identificar y priorizar rápidamente las acciones en los servidores y acelerar el tiempo de resolución
	Debe permitir la integración unificada de gestión automatizada y analítica de servidores, almacenamiento, protección de datos, convergencia e hiperconvergencia desde un único portal.
Accesorio	Incluir cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros
Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

B) SERVIDOR TIPO I	
Cantidad de Servidores	Siete (07) servidores
Factor de Forma	Blade (Formato Compatible con el chasis solicitado)
Procesador	Dos (02) procesadores de 16 núcleos, 2.9 GHz, 24M cache, de última generación con tecnología multi-threading.
Memoria RAM instalada	Mínimo 192GB, Dual Rank RDIMM 3200MHz ECC, Los módulos ofertados deberán ser de 16GB como mínimo. Capacidad de crecimiento mínimo de 2 TB. Capacidad de soportar memoria persistente
Discos de inicio	Dos (02) discos mínimos de 960Gb SSD en RAID 1. Debe soportar al menos 6 bahías de discos internos o a través de expansión interna, los cuales se podrán configurar en RAID 5.
Interfaces de Red LAN/SAN	Adaptador convergente con dos puertos (02) Ethernet de 10/25Gb con soporte FCoE offload.
Seguridad	Sistema de arranque (boot) seguro
	Bloqueo de sistema ante intento de cambios no autorizados o maliciosos de configuración y/o firmware.
	TPM 1.2/2.0 FIPS
	Contar con certificación encriptada de componentes del servidor que permita verificar que no hay componentes reemplazados o removidos una vez salidos de fábrica.
Administración	Sistema de administración y monitoreo a través de una sola consola gráfica basada en web para administración local y remota.
	Debe permitir visualizar el uso de recursos (CPU, memoria, almacenamiento interno)
	Debe soportar la agrupación de administradores para dispositivos específicos administrados (SBAC).
	Debe contar con soporte de RedFish
	Debe soportar OpenAPI spec v3
	Debe permitir el mapeo de consumo de energía por máquina virtual
	Debe contar con la capacidad de gestionar la garantía del servidor
Soporte de sistemas operativos certificados	Red Hat Enterprise Linux 6.x o superior, Windows Server 2019 o superior y VMWare ESXi 7.0 o superior
Garantia de sistemas operativos certificados	Red Hat Enterprise Linux, Windows Server y VMWare ESXi
Servicio de instalación	Servicio de instalación:
	- Los servidores deberán estar instalados dentro del Chasis y debidamente configurados
	Los servicios de instalación y puesta en marcha deben ser ejecutados por personal certificado del fabricante.
Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

C) LICENCIAS VIRTUALIZACIÓN Y ADMINISTRACION CENTRALIZADA	
Licencias de Virtualización	Licenciamiento para los siete (07) servidores solicitados. Licenciamiento perpetuo. Tipo OPEN. Versión Enterprise Plus o similar.
	Deberá ser una pieza de software denominada en el mercado "hypervisor" o capa de virtualización que se instale directamente sobre el Hardware sin necesidad de instalación de un Sistema operativo adicional para la ejecución de software de virtualización. (Bare Metal Hypervísor).
	Se debe incluir el software de administración centralizada para los servidores
Características	1. El hipervisor software de virtualización debe instalarse y ejecutarse directamente sobre los niveles más bajos de hardware de los equipos en modo BARE METAL sin necesidad de un sistema operativo anfitrión.
	2. Debe soportar particionamiento, es decir, debe tener la capacidad de creación y ejecución simultánea de múltiples máquinas virtuales sobre un mismo servidor físico, con soporte de sistemas operativos como Windows Server 2003, Windows Server 2008 R2 Standard/Enterprise, Windows Server 2012 R2 Standard/Datacenter, Windows Server 2016 Standard/Datacenter, Windows Server 2019 Standard/Datacenter y Red Hat Enterprise Linux 6.x y 7.x.
	3. Debe soportar aislamiento, es decir, que pueda asignar espacios independientes de CPU, RAM, disco duro y E/S a cada sistema operativo y controlar la asignación de recursos para cada máquina virtual.
	4. Debe soportar encapsulamiento, es decir, que todas las máquinas virtuales se administren como archivos y sean portables a través de copias.
	5. El hipervisor debe ser compatible con servidores basados en procesadores multi-núcleo compatibles con la arquitectura de 64 bits.
	6. La administración dinámica de la memoria física por parte del hipervisor debe tener las siguientes características:
	o Permitirá la sobresuscripción de la memoria física disponible a las máquinas virtuales, esto es, que la suma de la memoria asignada a las máquinas virtuales podrá ser mayor a la cantidad de memoria física.
	o Será capaz de trasladar automáticamente montos de memoria asignada, pero en desuso de una máquina virtual a otra.
	o Debe eliminar páginas de memoria redundantes de manera que 2 o más máquinas virtuales compartirán páginas de memoria idénticas entre ellas, evitando la necesidad de mantener copias redundantes.
	7. En caso el hipervisor propuesto no soporte la funcionalidad de sobresuscripción especificada en el punto anterior el Contratista / Proveedor debe ofertar 50% más memoria RAM en todos los servidores para suplir la falta de esta capacidad.
	8. Se requiere la capacidad de adicionar en línea interfaces de red virtual y dispositivos de almacenamiento virtual a máquinas virtuales que requieran una ampliación en sus capacidades de comunicación con la red IP o bien con la red de almacenamiento compartido.
	9. Capacidad de balanceo automático de cargas de trabajo que soportan los elementos físicos que la sustentan. Se requiere que dicho balanceo sea integral y comprenda los siguientes aspectos.
	o Balanceo de carga en la red IP: capacidad de utilizar protocolos de agrupación de interfaces de red para el balanceo de carga, en específico se requiere soporte a los protocolos LACP y Etherchannel.

C) LICENCIAS VIRTUALIZACIÓN Y ADMINISTRACION CENTRALIZADA	
	o Balanceo de carga del procesamiento. Se refiere a la capacidad de modificar la posición de las máquinas virtuales en referencia al elemento físico (servidor) que las sustenta, la infraestructura de virtualización debe ser capaz de reubicar automáticamente cualquier máquina virtual de forma que reciban suficientes ciclos de CPU y espacio real en la memoria RAM para cumplir con el nivel de servicio esperado.
	10. Se requiere que la plataforma de virtualización brinde una gestión dinámica de recursos para que se puedan crear contenedores de máquinas virtuales con recursos asignados (grupo de recursos), lo cual habilite a un usuario correr las máquinas virtuales requeridas, adicionar recursos dinámicamente para VM´s prioritarias y delegar el control de asignación de recursos hacia máquinas virtuales sin perder el control sobre el hardware. Así mismo que se pueda tener el control preciso de los recursos de los diferentes "grupos de recursos" y sus tamaños puedan ser modificados, que automatice la ubicación de una máquina virtual, que pueda balancear y optimizar cargas de trabajo y que reaccione a la adición o eliminación de recursos del clúster de las máquinas virtuales. Los grupos de recursos definidos no deberían estar asociados a servidores físicos, de manera que un mismo servidor físico pueda proporcionar recursos a varias agrupaciones de recursos. Posibilidad de definir políticas avanzadas de gestión de recursos para las máquinas virtuales en un solo servidor. Poder establecer un mínimo y máximo de recursos para CPU, memoria y ancho de banda de red y acceso a disco. Posibilidad de modificar esta asignación de recursos mientras las máquinas virtuales están corriendo. Posibilidad que las VMs adquieran más recursos de manera dinámica en situaciones de mayor demanda.
	11. Actualizaciones y parches de seguridad. Debe contar con un módulo para la administración e implementación de actualizaciones y parches de seguridad para el hipervisor, de manera que no interrumpa el funcionamiento y disponibilidad de las máquinas virtuales que corren sobre dichos hipervisores.
	12. Actualización de plataformas sin interrupción de servicio. Cuando sea necesario actualizar las plataformas del hipervisor en los sistemas operativos invitados, dicho proceso no será disruptivo sin requerir el reinicio de las máquinas virtuales.
	13. Seguridad en las máquinas virtuales. Posibilidad de utilizar un agente que habilite transferir las cargas de trabajo del procesador relacionadas con la ejecución de plataformas de seguridad de terceros como anti-virus y anti-spyware a un appliance virtual sin ejecutarse repetidamente dentro de las máquinas virtuales.
	14. Inicio de sesión único. La consola de administración de la plataforma debe solicitar las credenciales una sola vez para autenticar a los usuarios al acceder a todas las instancias o capas de administración de la misma. Debe ser basada en web, accesible desde un navegador web que habilite completar las tareas de administración de la plataforma de virtualización desde cualquier lugar que se acceda.
	15. Perfiles del hipervisor. Posibilidad de definir un perfil de referencia para todos los servidores físicos, de forma que se pueda verificar en cualquier momento un posible cambio de configuración en servidores físicos del entorno respecto a ese perfil o configuración de referencia para corregir dicha discrepancia.
	16. Debe soportar la definición de switches virtuales distribuidos de forma que se pueda hacer una definición de los switches y puertos de las máquinas virtuales a grupos de servidores físicos, de manera que dicha definición o configuración, sea consistente en todos los servidores físicos.

C) LICENCIAS VIRTUALIZACIÓN Y ADMINISTRACION CENTRALIZADA	
	17. Control de ancho de banda y asignación de QoS. Dado que las máquinas virtuales serán recolocadas en forma automática con fines de balanceo de cargas y continuidad de negocio, se requiere que los servicios de red puedan asignar un nivel de QoS así como un ancho de banda máximo permitido por cada máquina virtual o bien por perfil de máquina virtual y que este par de controles acompañen automáticamente a cada máquina virtual hacia cualquier servidor físico dentro de la infraestructura de virtualización conforme se mueva. Adicionalmente, el control de ancho de banda máximo debe ser bidireccional, es decir para tráfico IP que egresa e ingresa a cada máquina virtual.
	18. Conservación del estado de puertos virtuales: con el fin de mantener registros de la actividad de los puertos IP de las máquinas virtuales, es necesario que el estado de dichos puertos sea preservado aún en eventos de traslado de máquinas virtuales entre servidores físicos. De esta forma, debe conservarse el valor de los contadores de estadísticas asociadas a los puertos IP de las máquinas virtuales para que puedan ser usados en acciones de monitoreo y solución de fallas por parte de los administradores de la red IP integral (virtual y física).
	19. Teaming y balanceo de cargas de red. Capacidad de crear un “team” de NICs (tarjetas de red) en un host para proporcionar redundancia en caso de fallo de una de las tarjetas. Además, este team permite el balanceo de carga entre las tarjetas del team. Esta característica debe ser proporcionada por la plataforma de virtualización en lugar de requerir drivers de terceros que sólo soportan tarjetas específicas del fabricante de dichos drivers.
	20. Compatibilidad universal con tecnologías y protocolos estándares para el almacenamiento de datos. Los servicios de almacenamiento de la plataforma de virtualización deben ser compatibles con tecnología de almacenamiento tipo SAN con soporte para los protocolos ISCSI y/o FC, y de tipo NAS.
	21. Sistema de archivos de clúster. Los servicios de almacenamiento deben entregar el espacio en disco para almacenar la información de los sistemas operativos y los datos que estas últimas manipulan mediante un sistema de archivos y permitirá agregar o remover los nodos de dicho clúster sin interrumpir la funcionalidad de otros servidores o nodos de virtualización.
	22. El sistema de archivos de la plataforma de virtualización debe permitir que cualquier nodo del mismo tome el control de la ejecución de cualquier máquina virtual y por consecuencia también del servicio que esta sustenta. Con un servicio de almacenamiento compartido de esa forma, será posible balancear la carga dentro de la infraestructura virtual, así como mantener la disponibilidad de los servicios aun cuando falle alguno o varios de los servidores físicos que forman la capa física de la solución.
	23. El sistema de archivos de la plataforma de virtualización debe permitir el ajuste de los tamaños de los volúmenes, discos, archivos y bloques, de manera que habilite la optimización de la lectura y escritura de los sistemas operativos hospedadas en el mismo.
	24. Debe permitir el bloqueo de archivos en disco para asegurar que una misma máquina virtual no pueda ser prendida en múltiples servidores al mismo tiempo.
	25. Se requiere que el sistema de archivos también cuente con la característica de extenderse en forma dinámica una vez que los volúmenes físicos que hospedan al sistema de archivos han sido extendidos.

C) LICENCIAS VIRTUALIZACIÓN Y ADMINISTRACION CENTRALIZADA	
	26. El hipervisor debe ser capaz de reclamar espacio en disco utilizado por los sistemas operativos hospedados en las máquinas virtuales (VMs) de forma que cuando se han eliminado archivos dentro de una VM, el disco virtual de dicha VM pueda ser contraído y el espacio liberado sea retornado como espacio de disco libre hacia el depósito de VMs del hipervisor.
	27. Debe ser capaz de balancear de manera automática las cargas de los diferentes dispositivos de almacenamiento, determinando el mejor lugar para que vivan los datos de las máquinas virtuales.
	28. Debe ofrecer la capacidad de crear grupos y perfiles de almacenamiento de acuerdo a políticas definidas por el usuario, para que la selección del almacenamiento para nuevas máquinas virtuales sea más rápida y eficiente.
	29. Se deben poder asignar prioridades de acceso a los diferentes recursos de almacenamiento de acuerdo a reglas predeterminadas de negocio, para permitir preferencias del acceso al almacenamiento a VM´s críticas cuando haya contienda por los recursos.
	30. Opción de creación de discos thin para las máquinas virtuales en cualquier tipo de almacenamiento (FC ó ISCSI ó NFS) de forma que no sea necesaria la reserva de todo el espacio desde el principio. Con capacidad de monitoreo y alertas para prevenir la ocupación máxima de espacio en el disco físico.
	31. Debe ser capaz de realizar snapshot o imágenes en tiempo real de máquinas virtuales y restaurar dichos snapshots en un momento en el tiempo sin necesidad de detener las máquinas virtuales.
	32. Capacidad de establecer calidad de servicio en E/S a una misma unidad de disco, de forma que se pueda dar prioridad a las máquinas virtuales más críticas y poner límites a las menos importantes incluso en los momentos de congestión, e independientemente de en qué servidor físico corran.
	33. Posibilidad de asignar una tarjeta de E/S directamente a una máquina virtual, de modo que haga un “pass-through” del hipervisor y sea la máquina virtual la que tenga control de dicha tarjeta de E/S (tarjeta de red o HBA de disco).
	34. Las máquinas virtuales deben poder usar dispositivos USB conectados a un host físico. Esta conexión se debe mantener incluso si la máquina virtual se migra a otro host usando la migración en caliente.
	35. Debe permitir la evacuación automatizada y en línea de servidores físicos. Esta prestación debe ayudar a eliminar la necesidad de detener el servicio de las VM para poder realizar mantenimiento de los servidores físicos. Para lograr esto es necesario que sea posible dar la orden de evacuación de un servidor físico para que las máquinas virtuales empiecen a migrarse en línea a otros servidores. El orden de las migraciones y la selección del servidor físico destino debe ser determinado por un proceso automatizado que habilite hacer la evacuación en forma sistemática de forma que no haya impacto en el desempeño de las VMs en ejecución en los servidores físicos encargados de captar las máquinas virtuales que se están evacuando.
	36. Debe permitir la migración en línea del medio de almacenamiento. Al igual que con los servidores, la infraestructura de virtualización de servidores debe contar con la capacidad de permitir el mantenimiento o sustitución del medio de almacenamiento en disco donde residen los archivos de los sistemas operativos y datos que cada máquina virtual utiliza sin que haya interrupción en el funcionamiento de las máquinas virtuales.

C) LICENCIAS VIRTUALIZACIÓN Y ADMINISTRACION CENTRALIZADA	
	37. Debe permitir el reinicio automatizado de servicios ante la detección de fallas. Esta prestación debe proveer un servicio de monitoreo de signos vitales que comprenda dos ámbitos principales: el primero es el elemento físico de procesamiento (servidores) y el segundo ámbito son los sistemas operativos en ejecución dentro de las máquinas virtuales. El requerimiento es que la infraestructura de virtualización debe detectar fallas en cualquiera de dichos ámbitos y ejecutar una acción correctiva de forma automática.
	38. Debe tener detección de falla de elemento físico. Para el caso donde exista una falla en un elemento físico de procesamiento (servidor) que le impida continuar con la ejecución de máquinas virtuales, la infraestructura de virtualización debe detectar la pérdida de los signos vitales del elemento físico en cuestión y poner las máquinas virtuales afectadas nuevamente en ejecución sobre otros servidores físicos distribuyéndolas en forma sistemática y automática de forma que la carga de trabajo se dividida equilibradamente entre los servidores físicos que sigan funcionando correctamente.
	39. Debe contar con detección de falla de sistema operativo virtual. En el caso de falla en el sistema operativo en ejecución dentro de una máquina virtual que la lleve a un estado de “congelamiento”, debe ser capaz de detectar la pérdida de los signos vitales del sistema operativo e iniciar una acción de reinicio de dicha máquina virtual con el fin de poner el sistema operativo en funcionamiento nuevamente junto con la aplicación que éste sustenta.
	40. Debe permitir la restricción sobre máquinas virtuales para que sólo puedan residir en determinados hosts (que habilite el control de licencias asociadas a servidores físicos o a un número de CPUs concretas). Al mismo tiempo, poder definir qué máquinas virtuales pueden residir en un mismo servidor físico y cuáles tienen que forzosamente residir en diferentes servidores físicos.
	41. Debe permitir la configuración de cuotas que limiten el uso de los recursos de infraestructura como cómputo, memoria y almacenamiento.
Garantías del software	Se debe considerar cinco años**,** las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante o proveedor, de tal forma que en cualquier momento la entidad pueda reportar la incidencia, considerar un tiempo de respuesta de 4 horas.
Servicio de instalación	Servicio de instalación:
	01 Cluster de siete (07) servidores (nodos).
Garantías sobre la licencia del software de virtualización	30 horas por año para brindarle soporte a la plataforma de virtualización, durante el periodo de garantía

D) PLATAFORMA DE ADMINISTRACIÓN Y MONITOREO	
Características	1. Debe integrar herramientas de monitoreo y análisis de capacidad de cómputo, almacenamiento, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad.
	2. Se requiere que la plataforma colecte los datos sin intervención manual y sin necesidad de la instalación de agentes, con periodos de colección configurables.
	3. La plataforma debe ser capaz de integrarse de manera transparente con la infraestructura virtual, poder obtener los datos de un punto central de administración.
	4. Análisis Predictivo. La plataforma debe tener la capacidad de predecir y prevenir problemas relacionados con TI basado en modelos matemáticos y correlación del ambiente monitoreado.
	5. Correlación automática de objetos monitoreados: La plataforma debe ser capaz de correlacionar eventos que suceden en diferentes silos de tecnología, por ejemplo, cómo afecta la carga de máquinas virtuales a un hipervisor.
	6. Análisis de causa raíz. Análisis de infraestructura y operaciones de las máquinas virtuales que elimine el tiempo que consumen los procesos de resolución de problemas mediante un estudio automatizado de causa raíz.
	7. Aprendizaje en línea de carga en la infraestructura. La plataforma debe tener la capacidad de aprender del ambiente y ser capaz de distinguir la carga basándose en hechos históricos, como fin de mes, día de examen, etc. Esto con fin de poder identificar los periodos pico de rendimiento y en base a esto poder modificar los umbrales para poder determinar si se tiene un comportamiento esperado.
	8. Vistas Configurables. Debe proveer vistas de desempeño, capacidad y administración para diferentes métricas y objetos monitoreados, estas vistas deben tener la capacidad de ser configurables.
	9. Información clave. Los datos de desempeño deben ser abstraídos en medidas de carga, salud y capacidad que nos permitan identificar eficientemente problemas de desempeño con un menor esfuerzo.
	10. La plataforma debe proveer la capacidad auditar la configuración, grupos de usuarios y usuarios que la utilizan.
	11. Consola de trabajo: Consolas de trabajo en tiempo real que muestren información de desempeño, capacidad y de eventos de cambios de configuración de las máquinas virtuales. Esto debe permitir una administración proactiva y ayudarán a asegurar los acuerdos de nivel de servicio.
	12. Integración con ambientes virtuales. La plataforma debe integrarse de manera transparente y total con la instancia de administración central de la infraestructura.
	13. La solución debe proporcionar visibilidad completa en todos los niveles de infraestructura a través de una única consola de administración.
	14. La solución debe ser capaz de comprender la disponibilidad, el rendimiento, la utilización, los eventos, los registros y los cambios en cada capa de la infraestructura virtualizada, desde el hipervisor hasta los sistemas operativos.
	15. La plataforma de administración y monitoreo debe contar con alertas personalizadas y notificaciones de correo electrónico y SNMP.
	16. La plataforma debe tener la capacidad para generar reportes bajo demanda permitiendo al usuario configurar la información que se desea obtener.

D) PLATAFORMA DE ADMINISTRACIÓN Y MONITOREO	
	17. La plataforma debe permitir el control de acceso a la misma basado en roles.
	18. La plataforma debe tener capacidad de utilizar HTTPS para la comunicación entre sus componentes.
	19. La plataforma debe poder integrarse con servicios LDAP para control de usuarios
	20. Esta plataforma debe integrarse dentro de la consola de administración de la plataforma de virtualización.
	21. Debe administrar el cumplimiento de los hipervisores en base a políticas de hardening.
	22. La solución debe poder recopilar y analizar todos los tipos de datos logs generados por la máquina, por ejemplo, logs de rastreos de red, archivos de configuración, mensajes, datos de rendimiento, volcados de estado del sistema, etc.
	23. La solución debe poder agregar estructura a todos los tipos de datos de logs no estructurados, permitiendo a los administradores solucionar los problemas rápidamente, sin necesidad de conocer los datos de antemano.
	24. La solución debe ser capaz de proporcionar monitoreo, búsqueda y análisis de logs en tiempo real, junto con un panel de control para consultas almacenadas, informes y alertas, que permitan la correlación de eventos en múltiples niveles para la solución ofertada.
	25. El licenciamiento debe ser del tipo OPEN permitiendo contar con soporte del software en la modalidad 24x7 por cinco (05) años.

E) SOFTWARE DE ORQUESTACIÓN, AUTOSERVICIO Y APROVISIONAMIENTO	
Características	1. La interface para el auto aprovisionamiento debe soportar la integración con el directorio activo y certificados firmados por SSL, para el manejo de la autenticación de los usuarios de este.
	2. La interface para el auto aprovisionamiento debe soportar la gestión catálogo donde se puedan configurar plantillas de máquinas virtuales y las imágenes que se deseen poner a disposición de los usuarios del portal.
	3. Configuración de niveles de servicio. El software de orquestación debe incluir la capacidad de especificar diferentes niveles de servicio que estén relacionados con los recursos de la infraestructura para garantizar la asignación automática de recursos de procesamiento en función de dichos niveles de servicio
	4. La plataforma podrá ser capaz de organizar y entregar recursos de procesamiento, políticas, procesos y control granular de la administración al nivel de grupos de usuarios
	5. Debe soportar la configuración de catálogos de servicio que describan diferentes criterios de asignación de recursos, parámetros de configuración y procesos de automatización que controlen la manera en que las máquinas serán aprovisionadas y administradas durante todo su ciclo de vida (blueprints).
	6. La solución debe proporcionar un portal de autoservicio para el usuario a fin de ofrecer una experiencia de autoservicio personalizada.
	7. La plataforma debe contar con un módulo que registre todos los cambios que ha sufrido un recurso durante su ciclo de vida y el detalle de los usuarios que realizaron dichos cambios.
	8. La configuración de flujos de trabajo puede incluir uno o varios niveles de proceso de autorización.
	9. El diseñador de flujo de trabajo visual debe permitir que las actividades se inserten fácilmente en un flujo de trabajo. Debe proporcionar una interfaz visual de arrastrar y soltar para desarrollar flujos de trabajo personalizados.
	10. La solución debe contar con soporte para proporcionar un catálogo de servicios de TI unificado para aplicaciones e infraestructura.
	11. La plataforma debe aprovisionar infraestructura de manera automática.
	12. La solución debe contar con soporte para generar automáticamente planes de ejecución de implementación que permitan a la institución realizar auditorías antes de implementar aplicaciones reguladas
	13. El licenciamiento debe ser del tipo OPEN permitiendo contar con soporte del software en la modalidad 24x7 por cinco (05) años.

F) SOFTWARE DE VIRTUALIZACIÓN DE REDES Y VIRTUALIZACIÓN DE SEGURIDAD	
Características	- Deberá incluir las licencias de uso para todos los servidores o nodos.
	- El licenciamiento debe ser del tipo OPEN de manera que no esté asociado al servidor o nodo físico y permita su instalación en otro hardware de ser necesario (en el caso de reemplazo), contando además con derecho a actualizaciones y soporte directo del fabricante del software en la modalidad de 24x7.
	- Las licencias deberán quedar registradas a nombre de la Entidad.
	- Deberá entregar servicios virtuales de red y seguridad.
	- Se deberá gestionar a través de la misma consola centralizada de administración de la plataforma del software hipervisor.
	- Deberá poseer módulos de switching, routing y firewall stateful de capa 7.
	- Deberá soportar la creación de overlays basados en VXLAN o Geneve.
	- Deberá soportar bridge de VXLAN o Geneve – VLAN.
	- Deberá separar el plano de datos, control y administración
	- Deberá entregar alta disponibilidad en los componentes del plano de control
	- Deberá exponer una API para consumo de plataformas externas e integraciones
	- Deberá soportar mecanismos de Calidad de Servicio (QoS)
	- El componente de enrutador distribuido deberá tener separados los planos de datos y control, con soporte de rutas estáticas y BGP, soporte de bridging con el mundo físico, debe escalar horizontalmente, capacidad para enrutar el tráfico localmente en cada host.
	- Deberá soportar los siguientes protocolos de ruteo distribuidos en el hipervisor de cada servidor físico: BGP y rutas estáticas.
	- Deberá permitir la creación de balanceadores de carga virtuales.
	- Deberá implementar balanceo de cargas para tráfico TCP, UDP, HTTP y HTTPS por medio de uso de IP's virtiuales (VIPs).
	- Deberá implementar persistencia de sesiones, manteniendo la conexión de un cliente determinado con un mismo servidor durante la misma sesión.
	- El componte de balanceo de carga deberá implementar como mínimo, los siguientes algoritmos de balanceo: Round Robin, Weighted Round Robin, Least Connections y Weighted Least Connections.
	- El componente de firewall distribuido deberá ser stateful con capacidad de soportar integración con Active Directory para reglas basadas en usuarios y grupos. El componente debe estar en la capacidad de no terminar las sesiones en el momento del movimiento en vivo de una máquina virtual dentro del cluster y operar en espacio de kernel.
	- El firewall distribuido deberá ser transparente evitando configuraciones específicas de red, permitiendo protección dinámica de máquinas virtuales, incluso si se migran de servidor físicos.
	- El componente de firewall distribuido deberá estar en la capacidad de integrarse con soluciones de terceros para proporcionar servicios de Anti-Virus / Anti-Malware, IPS (Intrusion Prevention System), soportando reglas de asignación dinámica mediante el uso de etiquetas asociadas a las máquinas virtuales, garantizando la administración de políticas desde una única consola unificada.

F) SOFTWARE DE VIRTUALIZACIÓN DE REDES Y VIRTUALIZACIÓN DE SEGURIDAD	
	- Deberá permitir la traslación de direcciones IP mediante NAT e implementar servicios de asignaciones de direccionamiento IP dinámicamente.
	- Deberá soportar la configuración de VPN IPSEC.
	- Deberá permitir la Creación de respaldos de configuración automáticos.
	- Deberá de contar con funcionalidades de virtualización siendo compatible con soluciones de orquestación de contenedores Kubernetes.
	- Deberá soportar la integración con las nubes públicas Azure y AWS con el uso de un solo administrador o controlador centralizado.
	- Deberá implementar DHCP snooping y ARP snooping en las redes virtuales.
	- Deberá permitir la configuración de firewall en los elementos de ruteo de la solución (firewall de perímetro).
	- Deberá implementar la funcionalidad de L2VPN, permitiendo la extensión de capa 2 entre centros de datos.
	13. El licenciamiento debe ser del tipo OPEN permitiendo contar con soporte del software en la modalidad 24x7 por cinco (05) años.

G) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
Cantidad de Storage	Uno (01)
Factor de Forma	Rackeable
Tecnología	Storage con arquitectura unificada datos de bloques, archivos y VVols
Arquitectura	Arquitectura activa-activa de escalamiento vertical y horizontal con una disponibilidad del 99,9999% y sin punto único de falla.
	Debe admitir el uso de tecnología de discos NVMe y/o SSD y/o Flash de punto a punto con arquitecturas NVMe/FC, NVMe/TCP y vVOLs-over-NVMe.
Número de controladoras activas y redundantes entre si	El storage ofertado deberá tener mínimo dos (02) controladoras activas y configuradas en un cluster, intercambiables en caliente. El Contratista / Proveedor deberá considerar todos los elementos recomendados por el fabricante para la correcta configuración del cluster de controladoras. El storage ofertado deberá contar con la capacidad de escalar a al menos cuatro (04) controladoras formando un cluster.
	La configuración del storage deberá contar con al menos 80 cores y memoria cache de 512GB por cada par de controladoras.
	Deberá soportar protocolos FC
Conexión de cada controladora.	Las controladoras deberán soportar conectividad FC 16/32Gbps y iSCSI 10/25/100Gbps
	La configuración de cada controladora debe contar con al menos cuatro (4) puertos de 32Gbps para uso de protocolo FC nativo.
	Cada uno de los puertos FC indicados debe incluir un cable de fibra LC-LC de un mínimo de 5 metros de longitud, compatible con la solución.
	Debe contar con dos (2) puertos de 1GbE RJ45 para administración.
	Debe configurarse con al menos 2 números de puertos de backend SAS de 12 Gbps para ampliar la capacidad con gabinetes adicionales.
Conectividad Ethernet	El storage ofertado deberá incluir mínimo (02) puertos de 25GbE para tráfico NAS y (02) puertos de al menos 25GbE para replicación asíncrona.
Tipo de discos instalados y soportados	Debe soportar discos SSD o Flash y SCM basadas en NVMe. Todos los discos deben admitir almacenamiento persistente de datos.
	El storage debe proponerse y configurarse con mínimo 0.5 PB decimales de capacidad efectiva y debe soportar un máximo de 300,000 IOPS (tamaño de bloque de 8K, 70% de lectura, 30% escritura).
	La capacidad efectiva debe incluir funcionalidades de optimización de almacenamiento garantizadas por el fabricante de no menos de 1.8:1
	Se debe proporcionar una protección de datos usando los niveles de RAID soportados de acuerdo con las mejores prácticas del fabricante.
	Deben considerarse disco(s) o capacidad de reemplazo (spare) de acuerdo con las mejores prácticas del fabricante.
	El storage propuesto debe ser escalable a un mínimo de 200% mas de la capacidad configurada agregando discos de manera granular, bandejas adicionales y/o ampliando el cluster de controladoras.
Mantenimiento microcódigo de las controladoras	Los procesos de upgrade de microcódigo del arreglo de discos debe realizarse sin interrumpir el funcionamiento

G) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
Niveles de protección ante fallas de disco o Niveles de RAID soportados	El sistema como mínimo deberá soportar mecanismos de redundancia de datos dinámicos tipo RAID de paridad simple y doble que garantice la disponibilidad de los datos
Funcionalidades de eficiencia de uso de espacio	Debe admitir servicios de datos de clase empresarial activos incluidos siguientes:
	· Aprovisionamiento fino (thin provistioning)
	· Compresión y deduplicación en línea compatible con datos de bloques (FCP, iSCSI), archivos (CIFS, NFS) y VVOL.
	· Replicación asíncrona para bloques, archivos y vVOLs
	· Instantánea o snapshots en LUNs y de archivos NAS (con algoritmo ROW o similar que no requiera la preasignación de espacio para este fin), con capacidad de ser escribibles.
	· Clones o Clones delgados (thin).
	Para la réplica, cada controladora deberá de contar con dos puertos necesarios para esta funcionalidad a través de IP, de acuerdo con las mejores prácticas del fabricante.
Agrupación y protección de datos	Debe admitir la combinación de diferentes capacidades de discos en una sola agrupación o arreglo de almacenamiento y accesible para el par de controladores ofertados.
	El storage propuesto también debe admitir el crecimiento de la capacidad mediante el incremento de un solo disco para admitir actualizaciones granulares.
	El storage propuesto debe soportar la reconstrucción de datos a partir de múltiples discos utilizando RAID virtual.
Encriptación de datos	Debe incluir una solución de encriptación de datos en reposo basada en hardware) para cifrar los datos en todos los discos (AES de 256 bits) con gestión de claves automatizada incorporada. El cifrado debería funcionar a la perfección con todas las funciones de almacenamiento y sin ninguna penalización de rendimiento.
Integración a los servidores	El storage debe soportar la administración de multipathing y failover en la conectividad con los servidores, admitiendo las funcionalidades de MPIO de los sistemas operativos.
Calidad de Servicio	Debe incluir la funcionalidad de Calidad de Servicio (QoS) basado en prioridad de nivel LUN.
Integración con VMware y otros	El storage debe soportar las opciones de integración de VMware VAAI, SRM, VASA y VVOLs.
	Debe poder administrarse y provisionar servicios desde VCenter (QoS, replicación, políticas de snapshots)
	Soporte de ANSIBLE y Kubernetes CSI.
Administración, Monitoreo y Seguridad	La solución propuesta debe tener una herramienta de monitoreo y administración basada en la nube con soporte para dos (02) años de informes históricos. Debe ser capaz de generar reportes personalizados, monitoreo a tiempo real, análisis histórico de rendimiento para análisis y tendencias, y monitoreo de utilización de capacidad.
	Arranque seguro y protección contra actualizaciones de firmware no autorizadas para prevenir arranques maliciosos.

G) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
	Deberá 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.
Firmware	Los equipos ofertados deberán tener la capacidad de recibir actualizaciones del sistema operativo de las controladoras y de firmware de sus componentes, que el fabricante pueda liberar, sin costo adicional durante el tiempo que cubra la garantía.
Fuentes de Poder	Redundantes (Configuración N+1)
Ventiladores	Redundantes (Configuración N+1)
Accesorio	Incluir cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros
Licenciamiento de software de administración	Se debe incluir la licencia perpetua de software de administración, de interfaz gráfica. Esta licencia debe tener la cobertura para administrar la capacidad total soportada del storage sin limitar el número de servidores a conectar a este ni la cantidad de discos soportados por el arreglo. Debe tener también la capacidad de monitorear el nivel de rendimiento o performance del storage.
Servicio de instalación	Servicio de instalación:
	01 configuración inicial del storage
	01 creación de conexiones a los servidores Tipo 1 para el arranque del software de virtualización
	Los servicios de instalación y puesta en marcha deben ser ejecutados por personal certificado del fabricante.
Garantía por software	Se debe considerar un soporte por cinco (05) años, las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante o proveedor, de tal forma que en cualquier momento la entidad pueda reportar la incidencia, considerar un tiempo de respuesta de 4 horas.
	El soporte PROACTIVO debe ser del tipo 24x7 por cinco (05) años. Los servicios de soporte durante la garantía deben ser ejecutados directamente por el fabricante.
Garantía del Storage	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

H) SWITCHES FC	
Cantidad de Switches	Dos (02)
Factor de Forma	Rackeable de máximo 1U
Puertos Fibra Canal	Cada switch FC debe contar con 48 puertos FC 16/32 y 4 puertos QSFP, totalmente licenciados y habilitados con sus respectivos Transceiver de 32Gbps
Arquitectura	Full fabric.
Tipos de puertos soportados	D_Port, E_Port, EX_Port, F_Port, AE_Port; Modo Gateway: F_Port y NPIV-enabled N_Port
Clase de Servicio	Class 2, Class 3, Class F (Inter-switch Frames)
Fuentes de Poder	Redundantes y reemplazables en caliente
Administración	Herramientas avanzadas via web. SSH, Auditoría, Syslog NTP v3, CLI, REST API, HTTP, SNMP v1/v3
	Puerto de administración 10/100/1000 Mb/s Ethernet (RJ-45), In-band over Fibre Channel, un (1) puerto Serial (RJ-45) y un (1) puerto USB
Actualización de firmware	No disruptiva
Seguridad	DH-CHAP, autenticación FCAP; HTTPS, IPsec, IP filtering, RADIUS, TACACS+, RBAC, , SSH v2, SSL.
Garantía y Soporte	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

CAPACITACIONES	HORAS
Chasis Blade, Servidores Blade y Switch FC	24 horas
Storage All-flash	24 horas
Plataforma y Software de Virtualización	24 horas

Ítem 2: Equipamiento sede central - Solución de Ampliación de Capacidad de Almacenamiento

A) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
Cantidad de Storage	Uno (01)
Factor de Forma	Rackeable
Tecnología	Storage con arquitectura unificada datos de bloques, archivos y VVols
Arquitectura	Arquitectura activa-activa de escalamiento vertical y horizontal con una disponibilidad del 99,9999% y sin punto único de falla.
	Debe admitir el uso de tecnología de discos NVMe y/o SSD y/o Flash de punto a punto con arquitecturas NVMe/FC, NVMe/TCP y vVOLs-over-NVMe.
Número de controladoras activas y redundantes entre si	El storage ofertado deberá tener mínimo dos (02) controladoras activas y configuradas en un cluster, intercambiables en caliente. El Contratista / Proveedor deberá considerar todos los elementos recomendados por el fabricante para la correcta configuración del cluster de controladoras. El storage ofertado deberá contar con la capacidad de escalar a al menos cuatro (04) controladoras formando un cluster.
	La configuración del storage deberá contar con al menos 80 cores y memoria cache de 512GB por cada par de controladoras.
	Deberá soportar protocolos FC
Conexión de cada controladora.	Las controladoras deberán soportar conectividad FC 16/32Gbps y iSCSI 10/25/100Gbps
	La configuración de cada controladora debe contar con al menos cuatro (4) puertos de 32Gbps para uso de protocolo FC nativo.
	Cada uno de los puertos FC indicados debe incluir un cable de fibra LC-LC de un mínimo de 5 metros de longitud, compatible con la solución.
	Debe contar con dos (2) puertos de 1GbE RJ45 para administración.
	Debe configurarse con al menos 2 números de puertos de backend SAS de 12 Gbps para ampliar la capacidad con gabinetes adicionales.
Conectividad Ethernet	El storage ofertado deberá incluir mínimo (02) puertos de 25GbE para tráfico NAS y (02) puertos de al menos 25GbE para replicación asíncrona.
Tipo de discos instalados y soportados	Debe soportar discos SSD o Flash y SCM basadas en NVMe. Todos los discos deben admitir almacenamiento persistente de datos.
	La ampliación del storage debe proponerse y configurarse con mínimo 1.5 PB decimales de capacidad efectiva y debe soportar un máximo de 300,000 IOPS (tamaño de bloque de 8K, 70% de lectura, 30% escritura)..
	La capacidad efectiva debe incluir funcionalidades de optimización de almacenamiento garantizadas por el fabricante de no menos de 1.8:1
	Se debe proporcionar una protección de datos usando los niveles de RAID soportados de acuerdo con las mejores prácticas del fabricante.
	Deben considerarse disco(s) o capacidad de reemplazo (spare) de acuerdo con las mejores prácticas del fabricante.
	El storage propuesto debe ser escalable a un mínimo de 200% de la capacidad configurada agregando discos de manera granular, bandejas adicionales y/o ampliando el cluster de controladoras.

A) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
Mantenimiento microcódigo de las controladoras	Los procesos de upgrade de microcódigo del arreglo de discos debe realizarse sin interrumpir el funcionamiento
Niveles de protección ante fallas de disco o Niveles de RAID soportados	El sistema como mínimo deberá soportar mecanismos de redundancia de datos dinámicos tipo RAID de paridad simple y doble que garantice la disponibilidad de los datos
Funcionalidades de eficiencia de uso de espacio	Debe admitir servicios de datos de clase empresarial activos incluidos siguientes:
	· Aprovisionamiento fino (thin provistioning)
	· Compresión y deduplicación en línea compatible con datos de bloques (FCP, iSCSI), archivos (CIFS, NFS) y VVOL.
	· Replicación asíncrona para bloques, archivos y vVOLs
	· Instantánea o snapshots en LUNs y de archivos NAS (con algoritmo ROW o similar que no requiera la preasignación de espacio para este fin), con capacidad de ser escribibles.
	· Clones o Clones delgados (thin).
	Para la réplica, cada controladora deberá de contar con dos puertos necesarios para esta funcionalidad a través de IP, de acuerdo con las mejores prácticas del fabricante.
Agrupación y protección de datos	Debe admitir la combinación de diferentes capacidades de discos en una sola agrupación o arreglo de almacenamiento y accesible para el par de controladores ofertados.
	El storage propuesto también debe admitir el crecimiento de la capacidad mediante el incremento de un solo disco para admitir actualizaciones granulares.
	El storage propuesto debe soportar la reconstrucción de datos a partir de múltiples discos utilizando RAID virtual.
Encriptación de datos	Debe incluir una solución de encriptación de datos en reposo basada en hardware) para cifrar los datos en todos los discos (AES de 256 bits) con gestión de claves automatizada incorporada. El cifrado debería funcionar a la perfección con todas las funciones de almacenamiento y sin ninguna penalización de rendimiento.
Integración a los servidores	El storage debe soportar la administración de multipathing y failover en la conectividad con los servidores, admitiendo las funcionalidades de MPIO de los sistemas operativos.
Calidad de Servicio	Debe incluir la funcionalidad de Calidad de Servicio (QoS) basado en prioridad de nivel LUN.
Integración con VMware y otros	El storage debe soportar las opciones de integración de VMware VAAI, SRM, VASA y VVOLs.
	Debe poder administrarse y provisionar servicios desde VCenter (QoS, replicación, políticas de snapshots)
	Soporte de ANSIBLE y Kubernetes CSI.
Administración, Monitoreo y Seguridad	La solución propuesta debe tener una herramienta de monitoreo y administración basada en la nube con soporte para dos (02) años de informes históricos. Debe ser capaz de generar reportes personalizados, monitoreo a tiempo real, análisis histórico de rendimiento para análisis y tendencias, y monitoreo de utilización de capacidad.
	Arranque seguro y protección contra actualizaciones de firmware no autorizadas para prevenir arranques maliciosos.

A) ALMACENAMIENTO (STORAGE - Servidor TIPO II) - All-Flash	
	Deberá 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.
Firmware	Los equipos ofertados deberán tener la capacidad de recibir actualizaciones del sistema operativo de las controladoras y de firmware de sus componentes, que el fabricante pueda liberar, sin costo adicional durante el tiempo que cubra la garantía.
Fuentes de Poder	Redundantes (Configuración N+1)
Ventiladores	Redundantes (Configuración N+1)
Accesorio	Incluir cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros
Licenciamiento de software de administración	Se debe incluir la licencia perpetua de software de administración, de interfaz gráfica. Esta licencia debe tener la cobertura para administrar la capacidad total soportada del storage sin limitar el número de servidores a conectar a este ni la cantidad de discos soportados por el arreglo. Debe tener también la capacidad de monitorear el nivel de rendimiento o performance del storage.
Servicio de instalación	Servicios de instalación:
	01 configuración inicial del storage
	01 creación de conexiones a los servidores Tipo 1 para el arranque del software de virtualización
	Los servicios de instalación y puesta en marcha deben ser ejecutados por personal certificado del fabricante.
Garantía por software	Se debe considerar un soporte por cinco (05) años, las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante o proveedor, de tal forma que en cualquier momento la entidad pueda reportar la incidencia, considerar un tiempo de respuesta de 4 horas.
	El soporte PROACTIVO debe ser del tipo 24x7 por cinco (05) años. Los servicios de soporte durante la garantía deben ser ejecutados directamente por el fabricante.
Garantía del Storage	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

Ítem 3: Equipamiento sede central – Solución de Respaldo de la Solución de Servidores y Storage

A) SERVIDOR DE RESPALDO	
Cantidad de Servidores	Uno (01)
Factor de Forma	Rackeable maximo 2U, debe incluir rieles para montaje en Rack
Procesador	Dos (02) procesadores de 12 núcleos, 2.1 GHz, 18M cache
Memoria RAM instalada	Mínimo 128GB, RAM DDR4, Capacidad de crecimiento mínimo de 1 TB, configurado de manera balanceada
Capacidad de Almacenamiento	2 discos SSD M.2 de 480G en RAID-1 reemplazable en caliente
	Deberá contar con 8 discos de al menos 1.8TB SAS 10K rpm 12Gbps en RAID-5, reemplazables en caliente.
Controlador RAID	Controladora de Discos con 2GB de cache no volátil, RAID levels 0,1,10, 5 y 6.
Sistema Operativo instalado	Windows Server Estandar 2019 o superior pre-instalado de fábrica.
Interfaces de Red	Dos puertos 10/25 SFP28 integrados o embebidos o en una tarjeta de red.
	4 puertos de16/32Gbps Fibra Canal
Fuente de Poder	Fuente redundante Hot Swap o Hot Plug
Administración	Deberá contar con 1 puerto RJ45 de 1Gbps dedicado para la administración remota, con capacidad de acceso seguro, permitiendo que el servidor bloquee intentos de modificación de su configuración o cambios en el firmware por usuarios no autorizados o maliciosos.
	El servidor debe soportar monitoreo y registrar los cambios en el hardware y configuración de sistema.
	Debe soportar integración con RESTful API.
	El sistema de administración debe proveer acceso basado en roles
	Debe proveer alertas proactivas ante fallas en componentes críticos como CPU, Memoria y Discos Duros.
	Deberá permitir proactivamente a identificar si la BIOS, drivers, o lo agentes de administración de servidor están obsoletos y deberá permitir la actualización remota de los componentes de software/firmware
Software Instalados y licenciados	Sistema Operativo y solución de storage ofertada en el Item1, licenciamiento que debe ser soportado por el software de virtualización y el software de almacenamiento.
Accesorio	Incluir cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros
Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.

A) SERVIDOR DE RESPALDO	
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

B) LIBRERIA DE RESPALDO	
Cantidad de librería de respaldo	Uno (01)
Factor de Forma	Rackeable maximo 3U, debe incluir rieles para montaje en Rack. En caso de ser necesario se podra incluir modulos de expansión de 3U cada uno
Cantidad de Slots para cartuchos	120
Cantidad de dispositivos para tape	Ocho (08) Drives Ultrium LTO 9 FC
Unidades de Tape soportadas	LTO-9
Cartuchos	Se deberá incluir 12 cartucho LTO-9 y un cartucho de limpieza
Licencia de failover	Debe incluir la capacidad de soportar el control de rutas y balanceo de carga hacia los drives
Capacidad de encriptación	Licencia de activación incluida para cifrado administrado por aplicaciones y por libraría.
Fuentes de Poder	Redundantes y reemplazables en caliente.
Accesorio	Incluir cables de poder, cables FC de 5m mínimo, y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros.
Instalación	Instalación y puesta en marcha realizada por el fabricante del equipo
Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

C) SOFTWARE DE ADMINISTRACION DE RESPALDO	
Cantidad	Se debe considerar licenciamiento de backup para todos los equipos solicitados en el presente concurso
Propiedad de la Licencia	Se debe remitir el documento que indique claramente la propiedad de las licencias del software a nombre del Ministerio de Justicia y Derechos Humanos.
Capacidad requerida	Está preparada para realizar el respaldo y recuperación de los servidores virtuales y físicos de la solución.
Licenciamiento y soporte	Soporte por el periodo de Cinco (05) años 24x7
Solución de Respaldo - Generalidades	La solución deberá realizar respaldo a servidores físicos con los sistemas operativos: Linux y Windows y virtualizados con VMware, además de servidores con bases de datos Oracle y MS-SQL Server
	La solución deberá realizar el respaldo hacia cintas, librerías virtuales y almacenamiento de backup.
	Permitir respaldo por SAN y/o LAN de uno o más clientes, enviando sus datos a través de uno o más servidores de respaldo intermediarios a través de conectividad optimizada desde el cliente directamente al almacenamiento.
	Poseer la capacidad de realizar el respaldo de Servidores de Archivos en formato sintético y sintético virtual.
	La solución deberá poseer la capacidad de realizar respaldo de múltiples flujos de datos provenientes de dispositivos NAS (multiplexación) para Tape a través del protocolo NDMP
	Poseer la capacidad de recuperación de objetos y atributos de Active Directory a partir del backup del system state, sin la necesidad de rutinas de backup adicionales.
Características de la solución para la toma de backup de los servidores virtuales	La solución de respaldo no deberá necesitar de la instalación de agentes para poder realizar sus tareas de respaldo, recuperación y replicación de máquinas virtuales. Podrán instalarse agentes para el caso de recuperaciones granulares.
	La solución de respaldo debe incluir la instalación de agentes para la toma de backup de ambientes físicos.
	La solución de respaldo deberá ser capaz de comprender las máquinas virtuales como objetos del entorno virtual y respaldar las configuraciones de estas, al margen de los datos propios de las máquinas.
	La solución de respaldo deberá tener la funcionalidad de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual.
	La solución de respaldo deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador.
	La solución de respaldo deberá ser una solución altamente eficaz y preparada para el futuro integrándose en forma extensiva, con las APIs de los fabricantes de infraestructura virtualizada, para la protección de datos.
	La solución de respaldo deberá poder realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una

C) SOFTWARE DE ADMINISTRACION DE RESPALDO	
	replicación más frecuente. De este modo logrando lo establecido respecto de la merma de performance.
	La solución deberá ofrecer múltiples estrategias y/u opciones de transporte de datos para las tareas de respaldo (backup) a saber:
	- Directamente desde el storage a través del Hypervisor I/O (Virtual Appliance).
	- Mediante el uso de la red local (LAN).
	La solución de respaldo deberá poder mantener un respaldo (backup) completo sintético eliminando así la necesidad de realizar respaldo (backup) completos (full) periódicos ya que proporcionará un respaldo (backup) incremental permanente con lo que se permita ahorrar tiempo y espacio.
	La solución de respaldo (via el almacenamiento y/o el SW de backup) deberá contar con la tecnología de deduplicación para lograr un ahorro de espacio de almacenamiento para los respaldos (backup) integrándose con el almacenamiento de respaldo ofertado.
	La solución de respaldo deberá proveer una estrategia de recuperación rápida que permita proveer/devolver el servicio a los usuarios casi inmediatamente y en forma sencilla. Dicha estrategia debe consistir en el inicio y encendido de la máquina virtual, que haya fallado, directamente desde el archivo de respaldo (backup) en el almacenamiento habitual del respaldo (backup).
	Se deberá proveer la capacidad completar restauraciones completas del respaldo (backup) de cualquier máquina virtual dentro de una ventana de mantenimiento mínima, permitiendo completar los procesos de recuperación en suspensiones del servicio más cortas y menos frecuentes.
	Deberá poseer una opción de recuperación instantánea de archivos que se encuentren dentro de los respaldos (backup) de las máquinas virtuales. Lo que debe permitir acceder a los contenidos de los discos virtuales de dichas máquinas sin necesidad de recuperar el respaldo (backup) completo y reiniciar desde el mismo la máquina virtual.
	Deberá incluir un asistente para la recuperación instantánea a nivel de archivos en los sistemas de archivos más utilizados de Windows y Linux. Deberá poder crear un índice (catálogo) de todos los archivos que sean manejados por el sistema operativo Windows, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
	Deberá poder realizar búsquedas rápidas mediante índices de los archivos que sean manejados por un sistema operativo Windows, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
	Deberá asegurar la consistencia de aplicaciones transaccionales en forma automática por medio de la Integración con Microsoft VSS, dentro de sistemas operativos Windows.
	Deberá poder realizar el truncado de las bitácoras transaccionales (Transaction logs) para máquinas virtuales con Microsoft Exchange, SQL Server, Oracle directamente o a

C) SOFTWARE DE ADMINISTRACION DE RESPALDO	
	través del uso del uso del cliente/módulo para respaldo a nivel de aplicación.
	Deberá poder realizar notificaciones por correo, SNMP o a través de los atributos de la máquina virtual del resultado de la ejecución de sus trabajos.
	Se deberá poder recuperar a nivel granular cualquier aplicación virtualizada a nivel de VMware, en cualquier sistema operativo compatible (según matriz de compatibilidad), utilizando las herramientas de gestión de aplicaciones existentes.
	Deberá incluir herramientas de fácil recuperación guiada, mediante la cual los administradores de servidores de correo, tales como Microsoft Exchange versión 2013 y posteriores, puedan recuperar objetos individuales, tales como correos electrónicos y contactos, sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
	Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Microsoft SQL Server, puedan recuperar objetos individuales, tales como tablas y registros.
	Deberá incluir herramientas de fácil recuperación de elementos granulares de Microsoft Exchange 2013 en adelante, que no requiera inicializar la máquina virtual desde el respaldo y que pueda ser extraído en frio. (Ej. Correo, Citas de calendario, contactos, etc) y sin requerir infraestructura intermedia (“Staging”)
	Deberá ofrecer Trabajos de Copia de Backup con implementación de políticas de retención.
	Deberá incluir un Plug-in VMware para vSphere Web Client y poder monitorear la infraestructura de backup directamente desde el vSphere Web Client, con vistas detalladas y generales del estado de los trabajos y recursos de backup.
	Deberá soportar las últimas versiones disponibles de los hipervisores más populares de mercado a la fecha: VMWare vSphere 6.x o Superior.
	Deberá permitir la recuperación granular sin necesidad de montar ambientes temporales para:
	· Microsoft Active Directory
	· Microsoft Exchange Server 2013 en adelante.
	· Microsoft SQL Server 2017 en adelante
	Deberá ofrecer la posibilidad de almacenar los respaldos de forma encriptada, así como asegurar el tránsito de la información bajo este esquema.
	Deberá integrar una solución unificada de monitoreo de ambientes virtuales y respaldos de forma de poder co-relacionar ambas infraestructuras, las alarmas y reportes.
	Deberá ofrecer un conjunto de reportes capaces de presentar información de tipo:
	· Reportes que permitan la planificación de la capacidad.
	· Reportes que permitan la determinación de inefectividad en el uso de recursos.
	· Reportes que faciliten la visibilidad de tendencias negativas y anomalías.

C) SOFTWARE DE ADMINISTRACION DE RESPALDO	
	Deberá poseer la capacidad de generar segregación de acceso según el perfil del usuario, al monitoreo de la infraestructura conectada a la plataforma.
	Deberá ofrecer la capacidad de reportar el cumplimiento de políticas de protección de datos y disponibilidad acorde a parámetros definidos.
	Deberá incluir funciones de integración nativa (con o sin agentes) con Bases de Datos Oracle y MS SQL para recuperaciones granulares
Requerimientos de Administración y Seguridad	Deberá de poseer ambiente de administración de backup y restore a través de interfaz gráfica y línea de comando.
	Deberá de poseer interfaz web para administración, monitoreo, emisión de alertas, emisión de reportes sobre las operaciones de backup/restore y emisión de reportes sobre la capacidad y tendencia de crecimiento del ambiente; En caso de que existan múltiples ambientes de backup, una única interface web debe ser capaz de monitorear y agregar informaciones de diversos Servidores de Capa de Gerenciamiento para emisión de reportes.
	Poseer capacidad de establecer niveles de acceso diferenciados y configurables para actividades de administración y operación del software de backup:
	a. Permitir integración del control de acceso con sistemas de directorio Active Directory;
	b. Poseer mecanismo de auditoría, permitiendo la emisión de reportes donde consten, mínimo, los siguientes datos:
	· Fecha y hora de operación, usuario que realizó la operación, acción realizada (en caso de modificación de configuraciones, informar cual era la configuración anterior y la modificación realizada).
	c. Auditoría y control de acceso deben funcionar para operaciones realizadas vía interfaz gráfica y línea de comando.
	Poseer función de Schedule de respaldo a través de calendario y frecuencia;
	Permitir la programación de tareas de backup automatizadas y que sean definidos plazos de retención de los datos en las cintas magnéticas y dispositivos de disco;
	Poseer función para definición de prioridades de ejecución de Jobs de backup;
	Deberá permitir aplicar políticas de ciclo de vida de los datos;
	Administrar automáticamente y de manera centralizada la duplicación y movimientos de datos de backup entre los dispositivos de almacenamiento, posibilitando diferentes retenciones para cada copia.
	Deberá de poseer capacidad nativa de efectuar cifrado de los backups en 256 bits, en los Clientes de Backup y en dispositivos de media que soporten cifrado.
	Deberá de poseer la capacidad de administrar la duplicación y localización de medios de backup para fines de guardado externo, incluso fuera del sitio de la institución.
	Deberá de poseer la capacidad de automatizar los procedimientos de copia de cintas virtuales para cintas físicas a través de filtros personalizables.

C) SOFTWARE DE ADMINISTRACION DE RESPALDO	
Facilidades de Implementación y Mantenimiento	Poseer mecanismo de instalación de Clientes y Agentes de Backup de forma remota en cada uno de los clientes.
	Poseer mecanismos de actualización remota de los binarios de los Clientes y Agentes de Backup, por medio de un “wizard” o herramienta.
Recuperación de Desastres	Poseer de forma integrada y nativa la capacidad de Recuperación Automatizada del Sistema Operativo Windows sin necesidad de rutinas independientes de backup, no necesitando sistema operativo previamente instalado en el servidor de destino.
	Poseer la capacidad de recuperación del Sistema Operativo realizando boot PXE o CD/DVD.
	Poseer la capacidad de recuperación del Sistema Operativo en hardware diferente para ambientes Windows.
	Permitir búsqueda avanzada de datos protegidos, a través de Consola Web
Gestión de Reportes	La solución de protección debe tener reportes de riesgo que muestren en tiempos cuales son los servidores con más tiempo sin backup identificando los ambientes virtuales y físicos.
	La solución de recuperación de datos debe tener la capacidad de entregar reportes de gestión de respaldo y restauración de estas, informando el estado del respaldo y si fue satisfactorio, incompleto o fallido.
	La solución deberá estar en la capacidad de definir reportes estándar y configurables, que muestren gráficas y diagramas que simplifiquen el análisis, reporte y entendimiento de la situación e infraestructura de backup.
	La solución deberá tener una opción que permita construir reportes del rendimiento asociado al backup en los servidores y los medios de almacenamiento, dando la posibilidad de identificar problemas o cuellos de botella que estén afectando el rendimiento de la operación del backup.
	Reportes de bytes respaldados y recuperados en un periodo de tiempo por servidor.
	La solución deberá tener reportes para las máquinas virtuales protegidas y no protegidas en ambientes VMWare.
	La solución deberá tener reportes de uso de los dispositivos de backups (Ejem: Uso de cada Drive LTO7, LTO8), dependiendo de las funcionalidades de la librería de backup.
	La solución deberá tener reportes de throughput para los dispositivos de backups (Ejem: Uso de cada Drive LTO7), dependiendo de las funcionalidades de la librería de backup.
	La solución debe entregar reportes de comportamiento de toda la plataforma de backup durante la ventana de tiempo
	Reportes de inventario de servidores respaldados y que se le está respaldando, además de poder crear reportes nuevos que se puedan personalizar.
Garantía y soporte	Se debe considerar cinco (05) años 7x24, las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante o proveedor, de tal forma que en cualquier momento la entidad pueda reportar la incidencia, considerar un tiempo de respuesta de 4 horas.

D) STORAGE PARA RESPALDO A DISCO	
Cantidad de Dispositivo Dedicado a Respaldo a Disco	Uno (01)
Generalidades	La solución ofertada deberá ser un almacenamiento de propósito específico para datos de backup, con capacidad para guardar y retener copias de respaldo conforme a las políticas de backup definidas desde la aplicación de backup.
	Así, la solución debe estar certificada por el fabricante como solución de almacenamiento para backup. No se aceptarán soluciones que utilicen almacenamiento de propósito general que a través de controladores externas o software determinado emulen las capacidades de una solución propia para backup.
Características de Cómputo	El dispositivo almacenamiento mínimo deberá ser de una controladora, pudiendo ofertar 2 o más controladoras; por cada controladora se deberá tener mínimo 2 procesadores de 16 cores cada uno
	El dispositivo deberá tener mínimo 576 GB de memoria cache
Formato	El dispositivo debe permitir realizar el respaldo y recuperación de información basado en discos duros, mediante un mecanismo de optimización de deduplicación; dicha deduplicación deberá de realizarse en línea, durante la ingesta de los datos.
Grabación	Debe contar con la capacidad de emular y escribir en formato de tecnologías de cintas LTO.
	Debe soportar los protocolos CIFS y NFS para presentar volúmenes y realizar respaldos por SAN.
	Deberá de incluir protocolo de aceleración de respaldo, el cual permita duplicar el rendimiento de escritura de los datos.
Compatibilidad	El dispositivo debe ser compatible con los softwares de backup HPE Data Protector, EMC Networker e IBM TSM, Veeam, u otro equivalente.
Conectividad	La solución ofertada debe soportar conectividad Fibre Channel de 16/32Gb e Ethernet de 10Gb y 25Gb, teniendo como mínimo cuatro (04) puertos de 25GbE SFP28 y cuatro (04) puertos FC de 16/32Gb con sus respectivos Transceiver ópticos.
Disponibilidad	El dispositivo debe tener componentes como las fuentes de poder y ventiladores redundantes y reemplazables en caliente.
Tipo de Disco	La solución deberá soportar discos de tecnología SSD, SAS y NLSAS. Los discos duros que conforman esta solución deben ser de tipo SAS. Los discos de Estado Sólido (SSD) deben ser de una capacidad mínima de 3.84TB y los discos duros SAS deben ser de capacidad mínima de 8TB y una velocidad mínima de 7.2 K.
Rendimiento	El dispositivo deberá de poder llegar a un nivel de rendimiento de escritura de 57TB/hr.
Protección	La solución propuesta debe contar con el nivel de protección en RAID 6 en base a la tecnología y mejores prácticas del fabricante.

D) STORAGE PARA RESPALDO A DISCO	
Capacidad	El dispositivo deberá suministrarse con al menos 500 TB usables, debidamente licenciados. El dispositivo deberá suministrarse con una capa de aceleración basada en SSD con un mínimo de 5 discos SSD de 3.84TB
Deduplicación de Datos	La solución propuesta debe incluir la funcionalidad de deduplicación, el proceso debe correr en la solución y en ninguna circunstancia debe tener agentes o manejadores instalados en los servidores de respaldo o los clientes del Software de respaldo. La deduplicación deberá efectuarse en línea, durante la ingesta de datos.
	Debiendo estar licenciado para la capacidad de la solución propuesta/ofertada.
Administración	El dispositivo debe contar con un software de gestión propio que vía GUI o Web para su administración.
	Debe tener la capacidad de generar y enviar correos electrónicos o alarmas a una consola de gestión y soporte de SNMP Traps.
	Debe Permitir exportar información de monitoreo, log de errores, etc. hacia “fuera” del dispositivo.
	Especificar consumo eléctrico de la solución propuesta
Replicación	El dispositivo deberá de incluir la funcionalidad de réplica la información a través de redes IP de bajo ancho de banda a otro dispositivo igual, o de la misma familia.
Accesorio	Incluir cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, Transceiver y otros
Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo mínimo de cinco (05) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.
	Se debe considerar un Soporte Técnico anual del dispositivo, por el periodo de la garantía que es por mínimo de cinco (05) años.

CAPACITACIONES	HORAS
Solución de respaldo – Hardware	24 horas
Solución de respaldo – Software	24 horas

Nota: Con la finalidad de garantizar que la interconexión sea compatible, y facilitar el soporte y mantenimiento de la solución, de manera rápida y eficiente, es recomendable que los componentes del Hardware sean del mismo fabricante.

Los bienes (3 ítems), serán entregados e instalados, cumpliendo con las siguientes condiciones:

- ✓ Bajo la modalidad de Suma Alzada (a todo costo).
- ✓ Deben incluir un software de administración y monitoreo con licencia perpetua.

- ✓ Deben considerar componentes nuevos de primer uso, no siendo aceptados componentes reciclados, reensamblados o reacondicionados, tampoco se aceptarán aquellos que tengan denominación “refurbished” o su equivalente comercial.
- ✓ Deben ser instalados en los gabinetes indicados por MINJUSDH.
- ✓ Todo equipo antiguo y/o en desuso, a ser reemplazado, deberá ser retirado (conservando la integridad física del bien) debiendo ser entregado al personal técnico de la Oficina General de Tecnologías de Información del **MINJUSDH,** que será designado a requerimiento del Contratista / Proveedor.
- ✓ Deberán ser de la misma marca u homologados en su compatibilidad, y administrados por el mismo software de administración y monitoreo (sólo en el caso de Ítem 1 - “**Solución de Servidores y Storage”** e Ítem 2 - **“Solución de ampliación de Capacidad de Almacenamiento**”).
- ✓ Se precisa que la librería de respaldo no necesariamente deberá ser de la misma marca que los servidores y Storage (sólo en el caso de Ítem 3 - **“Solución de Respaldo de la Solución de Servidores y Storage**”).

❖ **INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO (**Para el caso de los 3 ítem´s “Solución de Servidores y Storage” y “Solución de Ampliación de Capacidad de Almacenamiento” y “Solución de Respaldo de la Solución de Servidores y Storage”.

- ✓ Por cuanto la modalidad de ejecución es Suma Alzada (a todo costo), el contratista debe realizar todas las actividades que pongan en correcta operación la solución en su conjunto por adquirir, de manera tal que se obtenga el mayor aprovechamiento del equipamiento y software.
- ✓ Será responsabilidad del Contratista efectuar las tareas necesarias de integración para la puesta en operación de la solución ofertada.
- ✓ La instalación, configuración y puesta en funcionamiento de la solución a nivel de equipos ofertados, debe ser realizada por personal debidamente certificado.
- ✓ La configuración de la solución a nivel de software de respaldo y software de virtualización debe ser realizada por personal experto certificado en la solución de software ofertada, en conjunto con el personal especialista que designe el Contratista / Proveedor.
- ✓ El contratista será responsable de la instalación, configuración de los componentes ofertados y será responsable de proporcionar todos los servicios, licencias, suscripciones, elementos y accesorios que sean necesarios para el correcto funcionamiento de toda la solución de producción.
- ✓ El contratista debe incluir en su propuesta los cables, accesorios correspondientes, y la interconexión entre dispositivos que permita la puesta en producción de la totalidad de la solución ofertada.
- ✓ La omisión en la oferta de algún bien o componente que al momento de la instalación y configuración resulte necesario para el normal funcionamiento de la solución ofertada o para el cumplimiento de las especificaciones técnicas ofrecidas, obligará al Contratista a proveerlo de inmediato y sin costo alguno para la Entidad, pues se entiende que la solución en su conjunto es una plataforma integral e interoperable para la provisión y gestión de servicios de computación, almacenamiento y redes.
- ✓ El Contratista / Proveedor deberá incluir una carta del fabricante del software de respaldo y software de virtualización en donde se indique que su propuesta del diseño, arquitectura, configuración e implementación de la plataforma de

virtualización, se encuentran alineados a sus mejores prácticas y recomendaciones técnicas.

- ✓ A la finalización correcta, la entidad debe emitir el acta de conformidad de Instalación, configuración y puesta en operación por cada ítem; conforme se describe líneas abajo.
- ✓ En la instalación y configuración, el contratista debe incluir obligatoriamente lo siguiente:
  - Montaje y energización de los componentes en los gabinetes provistos por la entidad.
  - Chequeo y remediación de los pre-requisitos mandatorios de hardware y software para el despliegue de la solución.

Para el caso del ítem 1 “Solución de Servidores y Storage” y de corresponder al caso del ítem 2 “Solución de Ampliación de Capacidad de Almacenamiento”, en relación a la Instalación, Configuración y Puesta En Funcionamiento, adicionalmente el contratista debe incluir obligatoriamente lo siguiente:

- Desplegar y configurar la infraestructura virtual para los servicios productivos de la entidad.
- Reservar los recursos necesarios para alojar los servicios de administración de la solución de producción. La misma se desplegará sobre los equipos ofertados, y contendrá los siguientes componentes: la herramienta de administración del entorno de virtualización, el gestor y los controladores de la red definida por software, almacenamiento definido por software, las herramientas de monitoreo y gestión de logs, la herramienta de orquestación y automatización de la solución ofertada.
- Configurará un ambiente para provisión de VMs, compuesto por: un (1) tenant o pool de recursos, un (1) grupo de red y/o un (1) catálogo de servicio, una (1) definición de una plantilla y/o patrón y/o mapa del tipo IaaS o equivalente que considere asignación de recursos, políticas de aprobación ó notificaciones de correo.
- Configurará el automatizador para que pueda generarse nombres personalizados a las máquinas virtuales. Se configurará hasta tres (3) campos para elegir la convención de nombres a utilizar en la máquina virtual a crear.
- Debe configurar un (1) perfil de red para la asignación de direcciones IPs.
- Debe configurar dos (2) conector de LDAP Active Directory y sincronización de los grupos de Directorio Activo para brindar acceso mediante roles a las herramientas o componentes de gestión de la solución ofertada, y sincronización de los grupos de Directorio Activo.
- Debe realizar la instalación del software de control de la red definida por software que permitan contar con alta disponibilidad de la interfaz de usuario, los servicios de API y la función central del plano de control.
- Debe registrar los nodos de transporte de datos recomendados.
- Desplegar los servicios de borde que comunicarán la red definida por software con la red tradicional.
- Desplegar los artefactos, los requerimientos, actividades que permitan procesar el tráfico entre la red física y la red lógica usando ruteo estático o dinámico (BGP).
- Replicar y Configurar hasta dos (02) segmentos o Switches lógicos de red capa 2 para máquinas virtuales y las VLAN correspondientes.
- Configurar dos (2) instancias de balanceador de carga por software.
- Configurar hasta dos (2) máquinas virtuales para conexión a una de las instancias creadas de balanceo de carga.
- Implementación de la funcionalidad de microsegmentación de redes definidas por software y configurada de acuerdo con indicaciones por la Unidad Usuaria.

- Realizará todas las integraciones necesarias entre todos los componentes y herramientas ofertadas para el correcto funcionamiento de la solución ofertada.
- Realizará (02) integraciones con las herramientas de administración del entorno de virtualización.
- Realizará una (01) integración con la herramienta de gestión de operaciones para que los logs puedan ser visualizados desde dicha herramienta.
- Construirá un (01) dashboard personalizado en la herramienta de gestión de logs.
- Creará un (01) query a medida en la herramienta de gestión de logs.
- Integrará la herramienta de gestión logs a un (01) servidor de correo electrónico.

Para el caso del ítem 3 “Solución de Respaldo de la Solución de Servidores y Storage”, en relación a la Instalación, Configuración y Puesta En Funcionamiento, adicionalmente el contratista debe incluir obligatoriamente lo siguiente:

- Desplegar y configurar la infraestructura virtual para los servicios productivos de la entidad.
- Proveer, instalar y configurar todo el equipamiento anteriormente mencionado.
- Configuración de los switches SAN y LAN del MINJUSDH para el nuevo equipamiento pueda comunicarse internamente.
- Configuración de integración con el hipervisor prexistente de la entidad con la solución de respaldo de información ofertada.
- Configuración de todo el licenciamiento de la solución de respaldo de información.
- El contratista instalará la última versión publicada (versión probada, no betas) de todos los firmwares, softwares y su respectivo licenciamiento.
- Todo cable de Fibra Óptica, UTP y Stack deberán ser provisto por el contratista en su totalidad.
- El MINJUSDH proveerá de servicio eléctrico y acondicionamiento a todo el equipamiento de la solución ofertada.
- Todo el licenciamiento del hardware y software del presente contrato deberá ser perpetuas y para gobierno, asimismo, deberá asegurar que todas las funcionalidades del software seguirán habilitadas posteriormente al vencimiento del contrato.
- En caso de que el licenciamiento no sea perpetuo, este deberá tener la misma vigencia que el servicio de soporte requerido.
- El contratista no debe realizar ninguna instalación o configuración del equipamiento anteriormente señalado hasta que dichos equipos estén debidamente etiquetados e inventariados por el MINJUSDH.
- Configuraciones y ejecución de respaldo de información en coordinación con el especialista del MINJUSDH.

VI. **PRESTACIONES ACCESORIAS. -** Aplicable para todos los ítem´s (1, 2 y 3).

SOPORTE TECNICO:

- Consiste en la verificación del correcto funcionamiento de los equipos suministrados por el contratista, mediante una gestión técnica permanente, ejecutando revisiones normalizadas para prever posibles fallos de funcionamiento, o proponer modificaciones adecuadas para asegurar el correcto funcionamiento; validando y manteniendo las últimas actualizaciones del software, firmware de las solución ofertada (esto, sobre la versión desplegada del producto al momento de la implementación), y que asegure

compatibilidad entre todos los componentes y el licenciamiento ofertado por el Contratista / Proveedor.

Además, contempla la atención a todas las alertas, logs o incidentes, que son inminentes a ocasionar u ocasionan una interrupción total o parcial de los componentes de la solución ofrecida, o que ocasionen un incidente en los sistemas de la entidad o un decremento en la calidad de este.

Estas pruebas deben efectuarse 1 vez al año, el primer mantenimiento debe ocurrir dentro de los 12 meses posteriores a la firma del acta de conformidad, y los subsecuentes dentro de los siguientes años que cobertura la garantía.

- El contratista deberá recepcionar los requerimientos de atención de soporte de la entidad, para lo cual deberá consignar un número de teléfono y correo de contacto para realizar dichos requerimientos.

  El equipamiento, así como las licencias del software deben incluir soporte de fábrica por un periodo de cinco (05) años.

  La solución (hardware y software) debe poseer soporte por parte del fabricante las 24 horas, durante los 7 días de la semana, incluido feriados, durante el período de cinco (05) años.

  El soporte en sitio deberá tener un tiempo de respuesta máximo de 4 horas para el personal y partes.

- Entre las actividades de garantía se debe contemplar mínimamente:

  - Creación de tickets vía telefónica.
  - Soporte técnico de la solución a cargo del fabricante.
  - Soporte técnico para asistir presencial o remotamente por medio de línea de contacto telefónico, correo electrónico y acceso remoto, en horario 24x7 durante el periodo de los cinco (05) años de garantía.
  - Ejecución, actualización de versiones de parches o fixes según indique o libere el fabricante, a fin de solucionar un inconveniente detectado en la plataforma.
  - La línea de contacto debe permitir la apertura de tickets tanto de soporte y garantía.
  - Todas las actualizaciones deberán ser provistas y certificadas por el fabricante de los equipos propuestos.

El contratista al finalizar cada Soporte Técnico, formulará un Informe de Mantenimiento, detallando las actividades realizadas, para la emisión del acta de conformidad de mantenimiento por parte de la entidad.

CAPACITACIÓN: Aplicable para el ítem 1 "**Solución de Servidores y Storage** e ítem 3 "**Solución de Respaldo de la Solución de Servidores y Storage**".

Item1:

CAPACITACIONES	HORAS
Chasis Blade, Servidores Blade y Switch FC	24 horas
Storage All-flash	24 horas
Plataforma y Software de Virtualización	24 horas

Item3:

CAPACITACIONES	HORAS
Solución de respaldo – Hardware	24 horas
Solución de respaldo – Software	24 horas

El Contratista / Proveedor brindará en total ciento veinte (120) horas de capacitación, para dictar capacitación sobre la configuración, implementación y administración de todos los componentes que forman parte de la solución implementada en el centro de datos, para cuatro (04) participantes, esta capacitación deberá considerar la emisión de una constancia para cada participante, y firmada por los especialistas certificados en la solución y/o componentes ofertados, y se llevará a cabo en las instalaciones de la Entidad o de forma virtual, previa coordinación con personal de la OGTI, el mismo que debe ejecutarse dentro del plazo de ejecución de cada ítem.

El personal encargado de brindar la capacitación por cada componente de la solución debe estar certificado por el fabricante a nivel de implementador según corresponda al componente sobre el cual se brindará la capacitación (puede considerarse varios capacitadores y puede presentarse al personal clave si es que éste satisface el requerimiento).

- Los Contratistas / Proveedores interesados, deberán presentar oferta por cada ítem; asimismo, están obligadas a presentar oferta por los **tres (3) ítems**, indicando el monto total propuesto.

- Un solo Contratista / Proveedor será seleccionado para la adjudicación de contrato de todos los ítems.

VII. Plazos de Entrega e Instalación.

Para el caso de los ítems 1y 3:

El plazo máximo total para la entrega e instalación de bienes es de ciento veinte (**120)** días calendario, contabilizados a partir del día siguiente de suscrito el contrato.

- Un máximo de cien (**100)** días calendario para la entrega de los bienes (equipamiento y de licencias de software), contabilizados a partir del día siguiente de suscrito el contrato.

- El Plazo de instalación de los bienes, implementación, despliegue, capacitación, servicios conexos y puesta en marcha de la solución será un máximo de quince (**15**) días calendario, contabilizados a partir del día siguiente la entrega de los

bienes por parte del Contratista / Proveedor, previa aprobación de la accesibilidad para instalación del bien.

-

- El Plazo de presentación del documento para la conformidad será un máximo de **cinco (05)** días calendario, contabilizados a partir del día siguiente de la culminación de la instalación y puesta en funcionamiento de los bienes.

Todas las acciones y/o actividades, previamente deberán ser coordinadas con la Oficina General de Tecnologías de Información del **MINJUSDH**.

Para el caso del ítem 2:

El plazo máximo total para la entrega e instalación de bienes es de ciento ochenta (**180)** días calendarios, contabilizados a partir del día siguiente de suscrito el contrato.

- Un máximo de cien sesenta (**160)** días calendario para la entrega de los bienes (equipamiento y de licencias de software), contabilizados a partir del día siguiente de suscrito el contrato.

- El Plazo de instalación de los bienes, implementación, despliegue, capacitación, servicios conexos y puesta en marcha de la solución será un máximo de quince (**15**) días calendario, contabilizados a partir del día siguiente la entrega de los bienes por parte del Contratista / Proveedor, previa aprobación de la accesibilidad para instalación del bien.

- El Plazo de presentación del documento para la conformidad será un máximo de cinco **(05)** días calendario, contabilizados a partir del día siguiente de la culminación de la instalación y puesta en funcionamiento de los bienes.

Todas las acciones y/o actividades, previamente deberán ser coordinadas con la Oficina General de Tecnologías de Información del **MINJUSDH**.

VIII. Documentos para la conformidad

El Contratista / Proveedor deberá presentar un documento conteniendo la siguiente información, según detalle:

Para el 1er Pago:

1. **Índice**

2. **Actividades ejecutadas**
   - Listado de actividades ejecutadas (Nombre de actividades con fechas de inicio y fin).
   - Listado de personal (Adjuntar seguros SCTR empleados).

3. **Entrega de Bienes**
   - Listado de bienes entregados (Hardware y Software, indicando la Marca, Modelo, Serie y otros).
   - Guía de remisión de bienes (Con el sello y firma de recepción).
   - Brochure o fichas técnicas de los bienes entregados (Elaborados por el fabricante de los bienes).

Para el 2do Pago:

1. **Índice**
2. **Actividades ejecutadas**
   - Detalle de actividades ejecutadas.
   - Listado de personal (Adjuntar seguros SCTR empleados).

3. **Instalación de Bienes**
   - Tomas fotográficas de la instalación e implementación.
   - Protocolo de funcionamiento o puesta en marcha.
   - Documento en donde detalle la capacitación y el soporte técnico.
   - Acta de conformidad, suscrita por el personal técnico de la Oficina General de Tecnologías de Información del **MINJUSDH.**
   - Tomas fotográficas situación final.
   - Diagrama de la arquitectura de la Solución Implementada.
   - Licenciamiento de la solución ofertada.
   - Inventario del total de equipos (hardware y software) de la presente contratación.
   - Manuales o procedimientos de la Solución Implementada.

Se deberá presentar un (01) ejemplar en versión física impresa y/o un (1) juego en versión digital en medio magnético (CD o DVD). asimismo, para el caso del ejemplar en digital deberá considerarse tolos los archivos fuente generados como parte del entregable.

IX. Requisitos del Contratista / Proveedor

Los Contratistas / Proveedores interesados, deberán presentar oferta por cada ítem; asimismo, están obligadas a presentar oferta por los tres (3) ítems, indicando el monto total propuesto.

Un solo Contratista / Proveedor será seleccionado para la adjudicación de contrato de todos los ítems.

➢ **Generales:**

El Contratista / Proveedor deberá:

- Persona Jurídica.
- Contar con registro Nacional de Proveedores – RNP
- Tener Registro Único del Contribuyente RUC: Estado: Activo y Habido
- Tener el Registro Único de Contribuyente – RUC, deberá encontrarse vinculado a su cuenta bancaria donde será destinado su pago.
- Indicar a una Persona de Contacto
- Indicar un Número Telefónico para contacto
- Indicar un Correo Electrónico para contacto
- La oferta debe ser presentado en Moneda Nacional - Soles (S/) e incluir todos los Impuestos, Seguros y cualquier otro tipo de cargo/monto que se incluya.
- Indicar si cumple con el 100% de las Especificaciones Técnicas.
- Ser distribuidor autorizado por los fabricantes de Hardware, sustentado con carta del fabricante.
- En la presentación de ofertas, el contratista deberá señalar la marca, modelo y número de parte, además deberá presentar Brochure y/o información técnica oficial, correspondiente al equipo ofertado

➢ **Específicos:**

A. Experiencia Especifica

- El Contratista / Proveedor deberá contar con una experiencia de tres (03) servicios de implementaciones de bienes relacionados al objetos de la contratación, en Centro de Datos y/o Cuartos de comunicaciones y/o

denominación similar, en los últimos 8 años a la fecha de presentación de la propuesta; el cual deberá ser acreditado con copia simple de contrato, órdenes de servicio y/o compra con sus respectivas constancias de conformidad y/o cualquier otro documento que acredite la realización del servicio satisfactoriamente.

B. Personal Clave

Requisitos del Personal Clave:

- **Un (01) Gerente de proyectos,** que cumpla con los siguientes requisitos**:**
  - ✓ Título Profesional en Ingeniería de Sistemas, Ingeniería de Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial y/o afines a las mencionadas.
  - ✓ Certificación oficial en Gerencia de proyectos - Project Management Professional (PMP) y/o SCRUM.
  - ✓ Experiencia laboral mínima de cinco (05) servicios, como gerente de proyectos similares al objeto de la convocatoria

- **Un (01) Arquitecto de la Solución,** que cumpla con los siguientes requisitos**:**
  - ✓ Profesional o Bachiller en Ingeniería de Sistemas, Ingeniería de Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial y/o afines a las mencionadas.
  - ✓ Debe contar con la certificación del fabricante de la solución ofertada, relacionado a temas de Arquitectura o Diseño de Datacenter virtualizado, ó del fabricante del equipamiento ofertado como Arquitecto de Servicios de Nube, nivel Experto.
  - ✓ Experiencia laboral mínima de cinco (05) servicios como arquitecto de soluciones similares al objeto de la convocatoria.

- **Dos (02) Implementadores de la Solución:**

  Para el caso del Item 1:

  Un (01) Implementador de Servidores y Storage

  - ✓ Profesional o Bachiller en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial y/o afines a las mencionadas.
  - ✓ Certificación oficial del fabricante en la solución de Servidores y Storage ofertada a nivel administrador u operación (o el equivalente de los mismos).
  - ✓ Experiencia laboral mínima de cinco (05) servicios como implementador de soluciones de Servidores y Storage.

  Para el caso del Item 3:

  Un (01) Implementador para Solución de Respaldo de la Solución de Servidores y Storage

  - ✓ Profesional o Bachiller en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial y/o afines a las mencionadas.

- ✓ Certificación oficial del fabricante en la solución de Respaldo de la Solución de Servidores y Storage ofertada a nivel administrador u operación (o el equivalente de los mismos).
- ✓ Experiencia laboral mínima de cinco (05) servicios como implementador de soluciones de respaldo o similares.

La formación académica, deberá ser acreditado con copia constancias y/o certificados de estudios y las experiencias laborales serán acreditadas con copia simple de contrato y/o órdenes de servicio con sus respectivas constancias de conformidad y/o cualquier otro documento que acredite la realización de servicios satisfactoriamente.

Cabe señalar, que, para la presentación de oferta, los Contratistas / Proveedores, podrán presentar Declaración Jurada del personal clave y de ser adjudicado para la firma de contrato deberán presentar el sustento de acuerdo a lo presentado en la oferta

X. Condiciones Adicionales

El Contratista / Proveedor se compromete a cumplir y a observar los “Lineamientos para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-COV-2”, establecidos en la Resolución Ministerial N°972-2020-MINSA y sus modificatorias o norma que la sustituya; asimismo se compromete a implementar los protocolos sanitarios necesarios, disposición que dicten los sectores y autoridades competentes. Asimismo, debe contar con el “Plan de Vigilancia, Prevención y Control de la COVID-19” el cual debe encontrarse registrado en el Sistema Integrado para COVID-19 (SICOVID-19) del Ministerio de Salud.
El Contratista / Proveedor deberá presentar para la suscripción del contrato, el registro de su “Plan de Vigilancia, Prevención y Control de la COVID-19”, en el Sistema Integrado para COVID-19 (SICOVID-19) del Ministerio de Salud.

Para acceder al **MINJUSDH**, el Contratista / Proveedor deberá presentar el resultado negativo de la prueba serológica o molecular, del personal de ingresará a los establecimientos penitenciarios para la instalación y configuración de los bienes.

XI. Conformidad

La conformidad de los bienes será dada por el/la coordinador/a de enlace y los responsables que dicho coordinador/a considere de las unidades orgánicas del MINJUSDH; previo informe técnico de la Oficina General de Tecnologías de Información del **MINJUSDH**.

XII. Supervisión

La supervisión y seguimiento de la ejecución del Contrato estará a cargo de la Oficina General de Tecnologías de Información del MINJUSDH

XIII. Forma de Pago y Condiciones de pago

La forma y condiciones de pago al Contratista en virtud del Contrato serán las siguientes:

i) **Anticipo:**
Hasta por un máximo del cuarenta (40%) del monto total del Contrato, se pagará dentro de los quince (15) días calendario, luego de que el Proveedor presente una solicitud formal al Comprador.

Dicha solicitud debe ser presentada dentro de los veinte (20) días calendario de suscrito el contrato.

La solicitud debe contener:

- Garantía Bancaria (Carta Fianza) por idéntico monto al solicitado como anticipo, la cual debe estar vigente por el plazo que cubra la amortización del anticipo otorgado, emitida por una institución bancaria o autorizada por la Superintendencia de Banca, Seguros y AFP y con corresponsalía en el Perú a favor de la Unidad Ejecutora 005 – Programa Mejoramiento de los Servicios de Justicia en Materia Penal en el Perú - PMSJMPP con las condiciones de solidaria, incondicional, irrevocable, de realización automática a solo requerimiento del Contratante.

- Comprobante de pago.

En el caso que el Proveedor solicite anticipo, la amortización del anticipo se realizará mediante descuento en proporciones iguales cada pago correspondiente.

ii) **Forma de Pago:**

El pago se realizará de acuerdo a las siguientes condiciones, luego que se haya emitido la respectiva conformidad.

Caso Ítem 1 y 3

N°	Producto / Entregable	Plazo Máximo	Monto S/.
1er Entregable	Entrega del equipamiento y de licencias de software	Hasta un máximo de **100** días calendario para la entrega de los bienes, contabilizados a partir del día siguiente de suscrito el contrato	80% del monto total de cada ítem ofertado
2do Entregable	Instalación, implementación, despliegue, capacitación, servicios conexos, puesta en marcha de la solución y presentación del documento para la conformidad	Hasta un máximo de **120** días calendario, contabilizados a partir del primer día hábil siguiente de suscrito el contrato.	20% del monto total de cada ítem ofertado

Caso Ítem 2

N°	Producto / Entregable	Plazo Máximo	Monto S/.
1er Entregable	Entrega del equipamiento	Hasta un máximo de **160** días calendario para la entrega de los bienes, contabilizados a partir del día siguiente de suscrito el contrato	80% del monto total de cada ítem ofertado
2do Entregable	instalación, implementación, despliegue, capacitación, servicios conexos, puesta en marcha de la solución y presentación del documento para la conformidad	Hasta un máximo de **180** días calendario, contabilizados a partir del primer día hábil siguiente de suscrito el contrato.	20% del monto total de cada ítem ofertado

Se efectuará el pago en soles dentro de los diez (10) días calendarios siguientes a la conformidad de cada entregable.

Para efectos de pago, se debe presentar una Carta dirigida al Programa la misma que debe ser presentada por mesa de partes presencial a nuestra Sede sito en Calle Manuel A. Fuentes N° 894, Urb. San Damián - San Isidro (si los comprobantes son manuales) o de forma virtual al correo mesadepartes@ejepenal.pe con copia al correo (si los comprobantes a presentar son electrónicos) adjuntar lo siguiente:

- Comprobante de pago.
- Formato CCI y Formato de Detracción (Según corresponda)
- Guía de remisión
- Documentos para la conformidad indicados en **numeral VIII**, del presente documento (Especificaciones Técnicas).

XIV. Garantía del Bien

Garantía del fabricante por cinco (05) años de reemplazo de partes o el bien, contados a partir del día siguiente de suscrita el acta de conformidad de instalación y puesta en funcionamiento.

- La garantía se solicitará a la solución de manera integral, y será de cinco (05) años, contado a partir del día siguiente de firmada el acta de conformidad de entrega de los equipos.
- Se solicitará al Contratista / Proveedor el procedimiento de escalamiento por garantía.
- Ante un RMA será de 24x7x365 hrs. (el componente de reemplazo debe entregarse dentro de las 4 horas posteriores a la orden del fabricante del reemplazo del mismo).
- Se solicitará al Contratista / Proveedor el procedimiento de solicitud de atención de soporte técnico.
- El Contratista / Proveedor deberá brindar lo requerido para la creación de ticket con el fabricante.
- El equipamiento, así como las licencias del software deben incluir soporte de fábrica por un periodo de cinco (05) años.
- El soporte en sitio deberá el personal y partes de los equipos

XV. Lugar de Entrega

Los bienes correspondientes a los Item1, Item2 e Item3, deberán ser entregados, instalados y configurados en las direcciones que se consignan, previa coordinación con la Oficina General de Tecnologías de Información del **MINJUSDH:**

ítem	Sede	Dirección	Bien
1	MINJUSDH – Sede Central	Scipión Llona 350, Miraflores - Perú	Los bienes correspondientes a los Item1, Item2 e Item3

XVI. Confidencialidad y Propiedad Intelectual

La información y documentación a la que tendrá acceso tiene carácter de confidencial siendo prohibido revelar dicha información a terceros. El Contratista deberá dar cumplimiento a todas las políticas y estándares definidos por la entidad en materia de seguridad de información, tanto de la información que se le entrega como la que genere durante la realización y a la conclusión de las actividades como informes, datos recopilados o recibidos. Todos los entregables elaborados dentro del contrato son de propiedad exclusiva de la Entidad, por lo que el contratista no podrá hacer uso de los mismos en forma total o parcial, fuera de la Entidad.

XVII. Responsabilidad del Contratista

El contratista será responsable por la calidad ofrecida y por los vicios ocultos, prestaciones y demás componentes relacionados a la contratación, por un plazo de un (01) año contado a partir de la conformidad por el cumplimiento de los aspectos técnicos y de la ejecución de las actividades del contrato, según lo indicado en el presente documento (Especificaciones técnicas).

Dicha conformidad no enerva el derecho a reclamar posteriormente por defectos y/o vicios ocultos.

XVIII. Penalidades

Si el Contratista / Proveedor incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, el Programa le aplicará automáticamente una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto de la contratación vigente o, de ser el caso, del monto del ítem que debió ejecutarse.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde:
F = 0.40 para plazos menores o iguales a sesenta (60) días o;
F = 0.25 para plazos mayores a sesenta (60) días;

Tanto el monto como el plazo se refieren, según corresponda, al contrato o Ítem que debió ejecutarse o, en caso de que estos involucraran obligaciones de ejecución periódica, a la presentación parcial que fuera materia de retraso.

Para efectos de la penalidad diaria se considera el monto del contrato vigente.

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. La calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo. El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado.

Finalmente, se cuenta con el derecho de exigir, además de la penalidad, el cumplimiento de la obligación.