



Especificaciones Técnicas para la Adquisición de un Sistema de Respaldo y Restauración para el Sistema de Índice Combinado de ADN

1. DENOMINACION DE LA CONTRATACIÓN

Adquisición de un Sistema de Respaldo y Restauración para el Sistema de Índice Combinado de ADN.

2. ANTECEDENTES

Con fecha 08 de julio de 2020, la República del Perú y el Banco Interamericano de Desarrollo (BID) suscribieron el Contrato N° 4959/OC-PE, cuyo objeto es contribuir a la financiación y ejecución del Programa "Mejoramiento de los servicios de justicia en materia penal en el Perú".

El objetivo general del programa es la mejora de la gestión del servicio del Sistema de Administración de Justicia Penal (SAJP), a través del: (i) aumento de la eficiencia del SAJP a través de los medios tecnológicos; (ii) aumento de la calidad de la investigación criminal; y (iii) mejoramiento del acceso a los servicios de administración de justicia penal a través de medios tecnológicos.

El principal impacto de la operación será mejorar la gestión del SAJP, medida en la disminución de la brecha entre procesos de investigación preliminar iniciados y resueltos

El Programa será ejecutado conjuntamente, por el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Ministerio Público (MP) y el Poder Judicial (PJ).

La Unidad Ejecutora 011, Carpeta Fiscal Electrónica, fue creada mediante Resolución de la Fiscalía de la Nación N° 1049-2020-MP-FN, y con Resolución de la Fiscalía de la Nación N° 1226-2020-MP-FN, se aprueba el Manual Operativo del Programa (MOP) "Mejoramiento de los servicios de justicia en materia penal en el Perú", en el cual se establece, entre otros, la descripción del Programa, beneficiarios, componentes del programa, marco institucional y ciclo operacional.

En ese contexto, la Oficina de Proyectos y Cooperación Técnica Internacional requiere de un Sistema de Respaldo y Restauración para la implementación del software "CODIS" que forma parte del Proyecto de Inversión denominado "**Creación del Centro Nacional de Perfiles Genéticos Humanos y fortalecimiento de los laboratorios de ADN de la Unidad de Biología Molecular y Genética de Lima y de las Unidades Médico Legales III de Arequipa y Lambayeque, del Instituto de Medicina Legal y Ciencias Forenses del Ministerio Público**".

3. FINALIDAD PÚBLICA

El presente proceso tiene por finalidad adquirir una Solución de Respaldo bajo las buenas practicas, en el cual se almacenará la data del Sistema de índice combinado de ADN, dicho esto se requiere contar con elementos de seguridad que protejan ante ataques informáticos.

4. CARACTERÍSTICAS TÉCNICAS

Se requiere contar con los siguientes sistemas necesarios para cumplir con la finalidad publica de la institución:



A continuación, se describe las características técnicas mínimas que deben cumplir, el cual se deberá incluir la instalación del equipamiento en la entidad:

SISTEMA DE RESPALDO Y RESTAURACIÓN

Se debe considerar:

- Un (01) Sistema de Almacenamiento de Respaldo en Discos cuyas características son las siguientes:

CARACTERÍSTICAS	DESCRIPCIÓN
Formato:	El dispositivo deberá ser un equipo de almacenamiento de propósito específico de respaldo de datos, no un equipo de almacenamiento de propósito general. El dispositivo debe permitir realizar el respaldo y recuperación de información basado en discos duros, mediante mecanismos de eficiencia de datos los que incluyen de compresión y 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 LAN. Deberá de incluir protocolo de aceleración de respaldo, el cual permita duplicar el rendimiento de escritura de los datos.
Conectividad:	La solución propuesta debe contar con un mínimo de 02 puertos Fibre Channel de 16Gb, 02 puertos Ethernet de 10Gb y 04 puertos Ethernet de 1Gb.
Disponibilidad:	El dispositivo debe tener componentes como las fuentes de poder y ventiladores redundantes y reemplazables en caliente.
Tipo de Disco:	Los discos duros que conforman esta solución deben ser de tipo SAS. Los discos duros SAS deben ser de capacidad mínima de 2TB y una velocidad mínima de 7.2 K.
Rendimiento	La librería virtual deberá de poder llegar a un nivel de rendimiento de escritura de 14TB/hr.
Crecimiento:	Debe permitir un crecimiento en TB sin deduplicación ni compresión de 48 TB RAW. El mismo se deberá realizar mediante la adición de nuevos cajones permitiendo un crecimiento modular de la solución.
Protección:	La solución propuesta debe contar con el nivel de protección en RAID 6, dicho RAID se deberá de realizar a nivel de hardware y no vía software.
Emulación	Deberá de tener la capacidad de emular como mínimo: 24 librerías virtuales 24,000 de cintas



Capacidad:	El dispositivo deberá suministrarse con al menos 24TB brutos sin deduplicar, debidamente licenciados.
De-Duplicación de datos::	La solución propuesta debe incluir la funcionalidad de Deduplicación, el proceso debe correr en la solución y bajo 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 VTL propuesta
Replicación:	Se debe incluir el licenciamiento para poder realizar la réplica entre los equipos ofertados. El dispositivo deberá de incluir la funcionalidad de réplica de la información de redes IP de bajo ancho de banda. La replicación debe soportar ser síncrona o asíncrona para los dos sistemas de almacenamiento solicitados y el equipo de almacenamiento para respaldo en disco.
Servicios de Instalación	Los servicios de instalación y puesta en marcha deben ser ejecutados directamente por el fabricante.
Seguridad	La solución deberá contar con la funcionalidad de protección de la información almacenada en un formato que impida la encriptación de los datos producto de ataques de ransomware asegurando la recuperación de los respaldos a su respectivo origen en caso este fuera afectado. Deberá soportar Encriptación validado de acuerdo con el estándar FIPS 140-2. Cumplir también con estándares de la industria en encriptación avanzada como AES-256
Servicios de notificación de eventos	El arreglo de discos debe contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos hacia el centro de soporte del fabricante.
Soporte	El soporte debe ser del tipo 24x7 por 03 años. Los servicios de soporte durante la garantía deben ser ejecutados directamente por el fabricante



Gestión Unificada	<p>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.</p> <p>Análisis del equipo conectada globalmente y utilizar estos datos para predecir y evitar problemas.</p> <p>Contar con capacidad de visualizar de forma remota tendencias detalladas de rendimiento, predicciones de capacidad, controles de estado e información de mejores prácticas.</p>
-------------------	--

CARACTERÍSTICAS	DESCRIPCIÓN
Software de Respaldo	Licenciamiento perpetuo para un (01) host físico de un (01) procesador.
Características	<p>El software para entornos virtuales debe de cumplir:</p> <ol style="list-style-type: none"> 1. La solución deberá incluir funcionalidades de respaldo (backup) y replicación integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada. 2. La solución no deberá necesitar de la instalación de agentes en el ambiente virtual o máquinas virtuales para poder realizar sus tareas de respaldo, recuperación granular y replicación de máquinas virtuales. 3. La solución no debe necesitar agentes para la recuperación granular de aplicaciones y archivos de los sistemas respaldados. 4. Deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar una merma en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto. 5. 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. 6. Deberá ser capaz de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual. 7. Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador. 8. 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. 9. 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 replicación más frecuente. De este modo logrando lo establecido respecto de la merma de performance. 10. La solución deberá ofrecer múltiples estrategias y opciones de transporte de datos para las tareas de respaldo (backup) a saber: <ol style="list-style-type: none"> 11. Directamente a través de Storage Area Network (SAN). 12. Directamente desde el storage a través del Hypervisor I/O (Virtual Appliance). 13. Mediante el uso de la red local (LAN). 14. Directamente de instantánea, con al menos un fabricante de sistemas de almacenamiento. 15. Directamente desde el repositorio NFS (Datastore NFS) 16. Deberá proporcionar un control centralizado del despliegue distribuido, para esto deberá incluir una consola web que provea una vista consolidada de su



	<p>despliegue distribuido y federación de múltiples servidores de respaldo (backup), informes centralizados, alertas consolidadas y restauración de auto servicio de máquinas virtuales y a nivel de sistema de archivos (granular), con asignación de permisos sobre máquinas virtuales individuales, y detección automática de permisos sobre máquinas virtuales acorde al perfil del usuario en la infraestructura virtual.</p> <ol style="list-style-type: none">17. 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.18. Deberá contar con la tecnología de deduplicación para lograr un ahorro de espacio de almacenamiento para los respaldos (backup).19. Deberá proporcionar protección casi continua de datos (nearCDP), que permita la reducción de los puntos objetivos de recuperación (RPO) sean mínimos.20. 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).21. La recuperación instantánea de las máquinas virtuales deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.22. Posterior a una recuperación rápida, se deberá poder realizar una restauración total sin interrupciones del servicio. La herramienta debe asegurar que el trabajo realizado por los usuarios no estará afecto al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción, sin imponer una restricción de tiempo en la ejecución de la máquina durante el proceso de recuperación instantánea.23. Se deberá proveer la capacidad realizar restauraciones completas del respaldo (backup) de cualquier máquina virtual dentro de una ventana de mantenimiento mínima, permitiendo completar los procesos de recuperación en interrupciones del servicio más cortas y menos frecuentes. La estrategia deber consistir en replicar o realizar una copia en caliente del respaldo (backup) de la máquina virtual que se encuentra en un almacenamiento de duplicado al almacenamiento en producción donde la máquina virtual ejecuta. Adicionalmente deberá poder transferir desde este estado de recuperación mediante más de un método tecnológico.24. Deberá poseer una opción de recuperación instantánea de archivos que se encuentren dentro de los respaldos (backup) y replicaciones 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.25. Deberá incluir un asistente para la recuperación instantánea a nivel de archivos en los sistemas de archivos más utilizados de Windows, Linux, Solaris, BSD o MacOS (Por lo menos 15 de ellos).26. Deberá poder crear un índice (catálogo) de todos los archivos que sean manejados por el sistema operativo Windows y Linux, sin agente, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).27. 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).
--	---



	<p>28. Deberá asegurar la consistencia de aplicaciones transaccionales en forma automática por medio de la Integración con Microsoft VSS, dentro de sistemas operativos Windows.</p> <p>29. Deberá poder realizar el truncado y respaldo de las bitácoras transaccionales (Transaction logs) para máquinas virtuales con Microsoft Exchange, SQL Server, Oracle sin el uso de agentes.</p> <p>30. 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.</p> <p>31. Se deberá poder recuperar a nivel de objetos de cualquier aplicación virtualizada, en cualquier sistema operativo, utilizando las herramientas de gestión de aplicaciones existentes.</p> <p>32. Deberá incluir herramientas de fácil recuperación guiada, mediante la cual los administradores de servidores de correo, tales como Microsoft Exchange versión 2007, 2010, 2013, 2016 y 2019 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. Sin requerir infraestructura intermedia ("Staging").</p> <p>33. Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de servicio de directorio, tales como, Microsoft Active Directory, pueden utilizar para recuperar objetos individuales, tales como usuarios, grupos, directivas de grupos (GPO), registros de DNS, particiones de configuración. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.</p> <p>34. 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. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.</p> <p>35. Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Oracle, puedan recuperar base de datos. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.</p> <p>36. Deberá ofrecer visibilidad instantánea, capacidades avanzadas de búsqueda y recuperación rápida de elementos individuales para Sharepoint 2010, 2013, 2016 y 2019 sin la utilización de agentes.</p> <p>37. Deberá poder ofrecer confiabilidad en un 100% en el inicio correcto de todas sus máquinas virtuales respaldadas y en el funcionamiento del rol que cumple dichas máquinas virtuales (DNS Server, Domain Controller, Mail Server, SQL Server, Oracle, etc) al momento de la recuperación, al poder realizar pruebas de recuperabilidad automatizadamente de las máquinas respaldadas.</p> <p>38. Deberá poder crear una copia de trabajo del entorno de producción de cualquier estado anterior para la resolución de problemas, pruebas de procedimientos, capacitación, etc. ejecutando una o varias máquinas virtuales desde el archivo de respaldo (backup) en un entorno aislado, sin necesidad de más espacio de almacenamiento y sin modificar el respaldo (backup).</p> <p>39. Deberá ofrecer el archivado en cinta, soportando VTL (Virtual Tape Libraries), biblioteca de cintas y drives independientes.</p> <p>40. Deberá ofrecer Trabajos de Copia de Backup y Archiving con implementación de políticas de retención. Con el objetivo de mantener una copia o replica de los archivos de respaldo a otro sitio en caso de desastre.</p> <p>41. 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.</p>
--	--



	<p>42. La solución debe tener un mecanismo de recuperación de emergencia de los respaldos cifrados por contraseña en caso de pérdida o extravío de la contraseña, pudiendo ser recuperada con una contraseña maestra generada vía Web.</p> <p>43. La solución debe tener un mecanismo de búsqueda global de archivo entre los respaldos.</p> <p>44. No deberá requerir hardware específico para alcanzar la deduplicación y compresión de la información fuera de los requerimientos estándar de cualquier software, y específicos para el caso.</p> <p>45. No deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.</p> <p>46. No deberá requerir licencias independientes para el respaldo y recuperación granular guiada y consistente de software:</p> <ul style="list-style-type: none">a) Microsoft Active Directory.b) Microsoft Exchange Server 2010 en adelante.c) Microsoft SQL Server 2008 en adelanted) Oracle Database 11.x y superior para Windows / Linuxe) Microsoft Sharepoint 2010 en adelante. <p>47. Deberá permitir la recuperación granular sin necesidad de montar ambientes temporales para:</p> <ul style="list-style-type: none">a) Microsoft Active Directory 2008 R2 en adelanteb) Microsoft Exchange Server 2010 en adelante.c) Microsoft SQL Server 2005 en adelanted) Oracle Database 11.x y superior para Windows / Linuxe) Microsoft Sharepoint 2010 en adelante. <p>48. Deberá ser capaz de realizar replicas en otros sitios o infraestructuras desde los respaldos realizados.</p> <p>49. Deberá presentar un método fácil de recuperación hacia ambientes de contingencia, con las acciones pre-configuradas para evitar acciones manuales en caso de desastre, similar a un botón de emergencia.</p> <p>50. Deberá ofrecer la posibilidad de almacenar los respaldos de forma cifrada, así como asegurar el tránsito de la información bajo este esquema desde el archivo de respaldo, sin requerir cifrado desde el sistema de almacenamiento.</p> <p>51. Deberá disponer de funcionalidades integradas que permitan la selección de un destino de almacenamiento de respaldos que pueda estar alojado en un proveedor de servicios en la nube (BaaS).</p> <p>52. Deberá disponer de funcionalidades integradas que permitan la selección de un destino de replica que pueda estar alojado en un proveedor de servicios en la nube (DRaaS).</p> <p>53. Capacidad de definir grupos de cintas magnéticas para ser utilizadas en una misma sesión de almacenamiento a cinta (Media Pool) para maximizar el rendimiento y velocidad de transferencia.</p> <p>54. La solución debe respaldar los archivos en cinta deduplicados, consiguiendo mayor eficiencia del espacio en cintas.</p> <p>55. El soporte del software y del hardware deben tener un único punto de contacto a fin de agilizar la solución de incidentes.</p> <p>56. Capacidad de procesar el envío de datos en múltiples unidades de cinta en paralelo para maximizar el ancho de banda y minimizar el tiempo de transferencia. • Capacidad de procesar múltiples trabajos de envío a cinta en paralelo hacia múltiples unidades de cinta.</p> <p>57. Capacidad de desacoplar el rol del servidor de la infraestructura de solución que permita el acceso a las unidades de cinta, evitando la necesidad que este rol se solape con otros roles de la solución.</p>
--	--



	<p>58. Capacidad de lectura directa desde el sistema central de almacenamiento, cuando en un entorno de infraestructura VMWare, este se encuentre presentado a través de protocolo NFS, evitando así, el paso de la información a través de las interfaces de control del hipervisor.</p> <p>59. Poder diferenciar, en máquinas virtuales Windows, aquellos bloques de disco que contengan datos irrelevantes (Dirty Blocks), y evitar su transferencia hacia los respaldos, así como la exclusión arbitraria de archivos dentro de máquinas virtuales Windows.</p> <p>60. La solución debe proveer mecanismos de protección para prevenir la sobre-exigencia sobre los sistemas de almacenamientos de la plataforma virtual, mediante el monitoreo proactivo de la latencia de los datastores, permitiendo la auto-regulación del sistema de respaldos y replicación en función de dichos umbrales definidos.</p> <p>61. Capacidad de diferenciar por unidad lógica o LUN y definir umbrales diferenciados para cada uno de ellos.</p> <p>62. Capacidad de aprovechar el subsistema Changed Block Tracking en el ambiente virtual, también para operaciones de vuelta atrás (fallback) acelerando la transferencia de datos al centro de datos productivo.</p> <p>63. La solución debe permitir el cumplimiento de estándares como GDPR para la eliminación de datos o registros de forma automatizada utilizando scripts (realizados por el cliente) dentro de los archivos de respaldo antes de restaurar una máquina virtual al ambiente productivo. Como también, permitir a los administradores realizar cambios en el sistema operativo, instalación o remoción de aplicaciones para cumplir con el cumplimiento corporativo cuando se restaure una máquina virtual.</p> <p>64. La solución debe integrarse con distintos Antivirus para realizar análisis de antivirus sobre los respaldos existentes en la plataforma, por ejemplo, respaldos anteriores de la misma solución, análisis antes de realizar una recuperación instantánea o completa de la máquina virtual. Como también integrarse en el mecanismo de prueba automatizado de las máquinas virtuales y/o del contenido de la máquina virtual, para realizar proactivamente análisis de antivirus.</p> <p>65. La solución debe identificar y excluir automáticamente los discos de las máquinas virtuales que cuenten con la característica "Multi-Writer" habilitada.</p> <p>66. Soporte para las plataformas de servidores Microsoft Windows Server 2019.</p> <p>67. La solución debe permitir publicar las bases de datos de servidores SQL soportados por la plataforma de forma granular directo hacia una instancia.</p> <p>68. Capacidad de recuperación de VMs y Respaldos de máquinas físicas con agentes de la plataforma (realizando la conversión automática de UEFI a BIOS en AWS) de forma directa a Amazon o Azure.</p> <p>69. La solución debe permitir cambiar los tipos de discos (Thin a Thick por ejemplo) cuando se requiera realizar replica de máquinas virtuales.</p> <p>La solución también debe permitir recuperar solo los bloques de discos de la máquina virtual que hayan cambiado utilizando CBT.</p>
--	---

- Se deberá considerar la instalación y configuración de hardware y software definido en coordinación con la oficina de Redes y Comunicaciones.

5. GARANTÍA COMERCIAL

La garantía del servidor en hardware se brindará durante el periodo de tres (03) años se iniciará desde la firma del acta de aceptación, y será brindado por el contratista avalado por la marca y con acceso al centro de asistencia técnica del fabricante.



El postor deberá ser representante y/o canal autorizado y/o partner del bien ofertado, para lo cual deberá adjuntar una copia de la carta del fabricante que lo acredite como representante y/o canal autorizado y/o partner de la marca ofertada del hardware ofertado a la presentación de ofertas con una antigüedad no mayor a 1 semana.

6. CONFIDENCIALIDAD

Toda información del MPFN a que tenga acceso el proveedor, así como su personal, es estrictamente confidencial. El proveedor y su personal deben comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito del MPFN.

7. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes y servicios ofertados por un plazo de tres (03) años, contados a partir de la conformidad otorgada por la entidad.

Las discrepancias referidas a defectos o vicios ocultos son sometidas a conciliación y/o arbitraje. El plazo de caducidad se computa a partir de la conformidad otorgada por la Entidad hasta treinta (30) días hábiles posteriores al vencimiento del plazo de responsabilidad del contratista previsto en el contrato.

8. LUGAR Y PLAZO DE ENTREGA DEL BIEN

El equipamiento deberá ingresar al almacén antes de empezar la instalación para su debida inspección técnica por parte del usuario. La entrega se realizará, previa coordinación con la Sub Gerencia de Almacén, en el Almacén Central del Ministerio Público, sito en Av. Abancay Cdra. 5 s/n sótano 1 – Cercado de Lima, en una (01) sola entrega. Los equipos serán entregados correctamente sellados en paquetes originales de la marca.

El plazo máximo de entrega será de Sesenta (60) días calendario, estos se calcularán desde el día siguiente de la suscripción del contrato.

El periodo de implementación comprende: la instalación, configuración, puesta en marcha y pruebas que se realizará en forma conjunta con la Oficina de Redes y Comunicaciones.

9. FORMA DE PAGO

El pago se realizará con la conformidad emitida por la Oficina Central de Tecnologías de la Información previo visto bueno de la Oficina de Redes y Comunicaciones. Se realizará el pago en un único pago. El pago se realizará de acuerdo con lo establecido en el artículo 171.1 del Reglamento de la Ley de Contrataciones del Estado.

10. CONFORMIDAD

La Sub Gerencia de Almacén otorgará la conformidad de recepción, contando previamente con el informe técnico de verificación emitido por la Oficina de Redes y comunicaciones. La conformidad de la implementación será emitida por la Oficina de Redes y Comunicaciones, quien será la responsable de la supervisión, una vez terminado la implementación y pruebas respectivas del cien por ciento (100%) del funcionamiento de los equipos. La conformidad se realizará de acuerdo con lo establecido en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

11. PENALIDAD

La Penalidad de los bienes se aplicará de acuerdo a lo establecido en el artículo 162° del Reglamento de la ley de Contrataciones del Estado.



En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = 0.10 \times \text{Monto Vigente} / F \times \text{Plazo vigente en días}$$

Donde F tiene los siguientes valores:

Para los plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F 0.40.

Para plazos mayores a sesenta (60) días:

- Para bienes, servicios en general y consultorías: F=0.25

12. MEDIDAS SANITARIAS

Para entrega en almacén y atenciones por garantía presenciales o para ejecución de traslados durante la ejecución del contrato, el proveedor será el responsable de garantizar que el personal asignado cumpla con los protocolos sanitarios conforme a lo dispuesto en el Decreto Supremo N° 080-2020-PCM y la Resolución Ministerial N° 972-2020-MINSA. los cuales son de aplicación obligatoria para la prestación de los servicios.

13. REQUISITOS DE CALIFICACIÓN

Para la calificación de propuesta se deberán considerar como requisitos:

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor debe acreditar un monto facturado acumulado equivalente a S/ 500,000.00 (Quinientos mil con 00/100 Soles) por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: Venta de Soluciones de Servidores de procesamiento, almacenamiento o respaldo.

B. EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

01 ESPECIALISTA DE SERVIDORES, quien ejecutará la instalación y configuración de solución de almacenamiento.

- Profesional en Ingeniería electrónico o sistemas o telecomunicaciones.
- Experiencia: Mínima de dos (02) años de experiencia como especialista de infraestructura de servidores.