ANEXO N° 01

OTASS	**FORMATO**	**Código:**	**FOR-UA-001**
	Especificaciones técnicas para bienes (Adquisición / Provisión)	**Versión:**	**03**

1.	**DETALLE DE LA SOLICITUD**			
	DENOMINACIÓN DE LA ADQUISICIÓN	ADQUISICIÓN DE LICENCIA DE SOFTWARE DE MONITOREO DE RED PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL OTASS		
	ACTIVIDAD DEL POI	AOI00158900145: ELABORACIÓN DE INFORMES DE OPERATIVIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA		
	META	90		
	FINALIDAD PUBLICA	Fortalecer la gestión, supervisión y continuidad operativa de la infraestructura tecnológica crítica de la Entidad, mediante la adquisición de una solución de software que permita monitorear de manera centralizada la disponibilidad, rendimiento y operación de los componentes de la infraestructura tecnológica tales como redes, servidores, aplicaciones y servicios. Dicha solución permitirá contar con sensores, alertas, reportes y mecanismos de seguimiento que faciliten la detección oportuna de incidentes, la atención preventiva de fallas, la reducción de tiempos de indisponibilidad y la mejora en la administración de los recursos tecnológicos que soportan los sistemas y servicios tecnológicos del OTASS.		
	OBJETO DE LA CONTRATACIÓN	Adquirir el licenciamiento de una solución de software de monitoreo de red, servidores, servicios y equipos críticos de comunicaciones, incluyendo los componentes necesarios para su uso, implementación, configuración, actualización, soporte técnico y puesta en operación; a fin de asegurar el seguimiento continuo del estado operativo de los componentes tecnológicos que soportan los sistemas y servicios tecnológicos del OTASS.		
2.	**PERSONAL DE CONTACTO QUE COORDINA CON LA UA Y EL/LA PROVEEDOR/A**			
	ORGANO/ UNIDAD ORGÁNICA	UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN		
	PERSONAL DE CONTACTO	ALAIN DONUHUE DONGO QUINTANA DANIEL MANUEL MINAYA CRUCES		
	CORREO ELECTRÓNICO	alain.dongo@otass.gob.pe daniel.minaya@otass.gob.pe	*CELULAR*	----------
3.	**VERIFICACION EN LAS SIGUIENTES PLATAFORMAS**			
	SI CUENTA CON FICHA DE HOMOLOGACIÓN APROBADA: (SI) O (NO)	NO CORRESPONDE		
	SI SE ENCUENTRA EN EL LISTADO DE BIENES COMUNES: (SI) O (NO)	NO CORRESPONDE		
	SI SE ENCUENTRA EN EL CATÁLOGO ELECTRÓNICO DE ACUERDO MARCO: (SI) O (NO)	NO CORRESPONDE		
	SI CUENTA CON NORMA TÉCNICAS: (SI) O (NO)	NO CORRESPONDE		
	SI CUNTA CON NORMA METROLÓGICAS: (SI) O NO)	NO CORRESPONDE		

4.	**CARACTERÍSTICAS Y CONDICIONES DEL BIEN**	
	CANTIDAD	Una (01) licencia de software de monitoreo de red
	UNIDAD DE MEDIDA (UNIDAD, CIENTOS, GALÓN, ETC.)	Unidad
	DIMENSIONES ((TAMAÑO, PESO,	NO CORRESPONDE

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

	VOLUMEN, ETC.)	
	CAPACIDAD (TENSIÓN, CORRIENTE, POTENCIA, RENDIMIENTO, VELOCIDAD, ETC.), EN CASO CORRESPONDA.	NO CORRESPONDE
	FORMA, COLOR, TEXTURAS.	NO CORRESPONDE
	MATERIAL (POR EJEMPLO: CUERO, TELA DE ALGODÓN, MADERA, METAL, FIERRO, MELANINE, ETC.).	NO CORRESPONDE
	CARACTERÍSTICAS PRINCIPALES	**CARACTERÍSTICAS MÍNIMAS DE LA LICENCIA DE SOFTWARE DE MONITOREO** La licencia de software de monitoreo debe contar con las siguientes características mínimas: 1) La solución deberá permitir el monitoreo de la infraestructura tecnológica de la Entidad, incluyendo equipos de comunicaciones, tales como switches, routers, access points, servidores físicos, servidores virtuales, servicios, aplicaciones, dispositivos de respaldo, almacenamiento y otros componentes críticos compatibles con los protocolos soportados por la herramienta. 2) La licencia o suscripción del software deberá ser registrada a nombre del OTASS. De requerirse una cuenta de correo electrónico institucional para el registro, activación, administración o notificación de licenciamiento, la cuenta de correo a emplear para dicho registro será licencias@otass.gob.pe. 3) La solución deberá contar con una interfaz de administración web, centralizada, intuitiva y accesible mediante navegador web. La interfaz deberá encontrarse en idioma español o, en su defecto, contar con documentación, soporte técnico o asistencia en idioma español. 4) La solución deberá permitir la administración de usuarios, perfiles o roles de acceso, a fin de diferenciar permisos de visualización, administración, configuración y generación de reportes, según las necesidades de la Entidad 5) La plataforma deberá poder implementarse en modalidad local u on-premise dentro de la infraestructura tecnológica de la Entidad. También podrá admitir componentes complementarios en la nube, siempre que ello no impida la operación principal local ni comprometa la seguridad, disponibilidad o confidencialidad de la información institucional 6) La licencia deberá permitir el monitoreo de hasta dos mil quinientos (2,500) sensores, métricas, monitores, elementos o unidades de medición equivalentes, según el esquema de licenciamiento del fabricante, debiendo garantizar la cobertura de la infraestructura tecnológica indicada por la Entidad. 7) Se aceptarán soluciones cuyo modelo de licenciamiento, suscripción, soporte o derecho de uso no se encuentre basado estrictamente en sensores, siempre que el proveedor garantice la capacidad de monitoreo requerida por la Entidad para hasta dos mil quinientos (2,500) sensores, métricas, ítems, monitores, checks, OID, interfaces, servicios, elementos supervisados o unidades de medición equivalentes, según la terminología y esquema técnico-comercial de la solución ofertada. 8) La solución deberá permitir la detección automática o asistida de dispositivos y servicios en la red, mediante protocolos estándares o mecanismos compatibles, tales como SNMP, ICMP, WMI, WinRM, SSH, API, agentes, Syslog, traps SNMP u otros equivalentes 9) La solución deberá contar con paneles de visualización o dashboards configurables, que permitan observar el estado de la infraestructura monitoreada con actualización periódica o en tiempo cercano al real, según los intervalos de sondeo configurados. 10) La solución deberá permitir la administración centralizada del monitoreo de equipos de comunicaciones, servidores, servicios, aplicaciones y demás elementos compatibles, incluyendo la configuración de sensores, umbrales, alertas, credenciales, grupos, mapas, vistas y reportes. 11) La solución deberá permitir la gestión de eventos, alertas y cambios detectados en la infraestructura monitoreada. En caso incluya funcionalidades de gestión de configuración de dispositivos de red, estas deberán permitir el registro, respaldo, comparación o control de cambios de configuración, conforme a la compatibilidad de cada equipo. 12) La solución deberá permitir, de manera nativa, mediante módulo complementario, integración soportada, componente adicional incluido en la oferta o procedimiento automatizado implementado por el proveedor, realizar el respaldo, registro, comparación o control de cambios de configuración de dispositivos de red compatibles, siempre que dichos equipos cuenten con los protocolos, permisos y credenciales requeridas.

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

		13) En caso la solución ofertada no cuente con funcionalidad nativa de gestión de configuración de dispositivos de red, el proveedor deberá indicar el mecanismo alternativo propuesto para el respaldo o control de cambios, el cual deberá estar incluido dentro de la oferta y no generar costos adicionales para la Entidad durante la vigencia contratada. **CARACTERÍSTICAS MÍNIMAS PARA EL MONITOREO INTEGRADO DE RED** 1. La solución deberá incluir funcionalidades de monitoreo de red integradas o módulos equivalentes que permitan supervisar la disponibilidad, estado y rendimiento de nodos, interfaces, enlaces, volúmenes, servicios y demás elementos compatibles. 2. La herramienta deberá permitir obtener reportes, gráficos y métricas históricas o en tiempo cercano al real, respecto de por lo menos los siguientes aspectos: • Disponibilidad de dispositivos, servicios e interfaces. • Tendencia histórica de los parámetros monitoreados. • Capacidad y utilización de ancho de banda. • Utilización de CPU, memoria, disco, almacenamiento o recursos equivalentes en equipos físicos y virtualizados. • Errores, descartes, tráfico broadcast, multicast y unicast en interfaces de red. • Latencia, pérdida de paquetes y tiempo de respuesta. • Estado de equipos, interfaces, enlaces, volúmenes, VLAN, servicios o componentes equivalentes. • Consumo de ancho de banda por dispositivo, interfaz, aplicación, protocolo, dirección IP u otros criterios disponibles según la fuente de datos. 3. La solución deberá permitir la generación de vistas gráficas, mapas o diagramas de la red, utilizando información obtenida por la propia herramienta y datos adicionales definidos por el usuario 4. La solución deberá permitir identificar visualmente los distintos tipos de elementos monitoreados, tales como switches, routers, servidores, access points, servicios, aplicaciones u otros, mediante iconos, etiquetas, categorías o elementos gráficos equivalentes. 5. La solución deberá permitir el descubrimiento automático o asistido de la red mediante protocolos estándares o mecanismos compatibles, tales como SNMP v1/v2c/v3, ICMP, WMI, WinRM, SSH, APIs, agentes u otros equivalentes, de acuerdo con rangos de direcciones, credenciales o parámetros definidos por la Entidad 6. La solución deberá permitir generar mapas, vistas o representaciones gráficas de la topología, mostrando conexiones, dependencias, relaciones lógicas o estados de los dispositivos, de acuerdo con la información disponible y la compatibilidad de los equipos monitoreados. 7. La solución deberá permitir la definición de grupos, categorías, etiquetas o contenedores lógicos para organizar dispositivos, aplicaciones, servicios, sedes, áreas o componentes tecnológicos, mostrando el estado consolidado de los elementos que los conforman. 8. La solución deberá permitir diferenciar visualmente, mediante colores, estados, iconos o indicadores equivalentes, el cumplimiento o superación de umbrales definidos para las variables monitoreadas. 9. La solución deberá permitir configurar vistas, paneles, dashboards o reportes personalizados, de acuerdo con las necesidades operativas de la Entidad. 10. La solución deberá permitir definir umbrales de operación para las variables monitoreadas y generar alertas cuando dichos umbrales sean superados durante un periodo determinado o bajo condiciones configurables 11. La solución deberá registrar información asociada a las alertas generadas, incluyendo fecha, hora, elemento afectado, métrica, condición detectada, severidad, estado y descripción del evento. 12. La solución deberá permitir configurar alertas basadas en una o más condiciones, métricas o umbrales, así como establecer reglas para evitar alertas repetitivas o falsas alarmas. 13. La solución deberá permitir monitorear access points o controladores inalámbricos compatibles, mostrando información como estado, dirección IP, dirección MAC, SSID, canal, clientes conectados, intensidad de señal u otros parámetros disponibles según la compatibilidad del fabricante. 14. La solución deberá permitir el monitoreo de parámetros relacionados con energía en equipos compatibles, tales como estado de fuentes de poder, consumo, PoE, temperatura, ventiladores, UPS u otros sensores disponibles. 15. La solución deberá permitir la configuración de umbrales manuales y, de contar con dicha funcionalidad, umbrales dinámicos o basados en comportamiento histórico, para alertas de advertencia y criticidad. 16. La solución deberá contar con herramientas de análisis de métricas que permitan comparar, correlacionar o visualizar diferentes

		indicadores de rendimiento, así como exportar información para análisis técnico. 17. La solución deberá permitir la integración o monitoreo de entornos físicos, virtuales, inalámbricos, SDN, controladores o plataformas administradas mediante protocolos estándares, APIs o mecanismos documentados por los fabricantes, siempre que dichos componentes formen parte de la infraestructura de la Entidad. **CARACTERÍSTICAS MÍNIMAS PARA EL MONITOREO DEL ANCHO DE BANDA Y ANÁLISIS DE TRÁFICO** 1. La solución deberá incluir funcionalidades nativas, módulos, colectores, integraciones, componentes complementarios o mecanismos equivalentes incluidos en la oferta, que permitan el monitoreo de ancho de banda, utilización de interfaces y, de corresponder, el análisis de tráfico de red. 2. La plataforma deberá permitir el monitoreo del tráfico y utilización de enlaces e interfaces mediante protocolos estándares, tales como SNMP, ICMP, APIs, agentes, colectores, sondas o mecanismos equivalentes. Asimismo, cuando los equipos de comunicaciones o fuentes de datos lo permitan, deberá poder integrarse con tecnologías de análisis de flujo, tales como NetFlow, sFlow, J-Flow, IPFIX u otros protocolos equivalentes, de acuerdo con la compatibilidad de los dispositivos y la arquitectura de la solución ofertada. 3. La solución deberá presentar la información de tráfico mediante gráficos, tablas, paneles o reportes de fácil interpretación, permitiendo identificar consumo por interfaz, dispositivo, dirección IP, aplicación, protocolo, puerto, conversación o criterio equivalente. 4. La solución deberá permitir visualizar información de tráfico en tiempo cercano al real, conforme a los intervalos de recolección configurados, así como consultar información histórica almacenada. 5. La solución deberá almacenar los datos recolectados en una base de datos, repositorio o mecanismo equivalente propio de la solución, permitiendo su consulta, análisis y generación de reportes. 6. La solución deberá permitir configurar los intervalos de recolección, actualización y retención de la información de tráfico, de acuerdo con la capacidad de la plataforma, mejores prácticas del fabricante y necesidades de la Entidad. 7. La solución deberá permitir el análisis de tráfico mediante protocolos estándares de flujo, tales como NetFlow v5/v9, sFlow, J-Flow, IPFIX o tecnologías equivalentes, de manera nativa o mediante colectores, integraciones, módulos o componentes complementarios incluidos en la oferta. El proveedor deberá precisar en su propuesta los protocolos soportados, la forma de integración, el alcance funcional y las condiciones de retención, visualización y generación de reportes. 8. La solución deberá permitir identificar patrones de uso de tráfico a través del tiempo, mediante gráficos, tendencias y reportes históricos. 9. La solución deberá integrar o correlacionar la información de tráfico con estadísticas de rendimiento de interfaces, tales como utilización, errores, descartes, estado operativo, velocidad, disponibilidad o métricas equivalentes. 10. La solución deberá permitir detectar, alertar o reportar comportamientos anómalos de tráfico, tales como incrementos inusuales de consumo, saturación de enlaces, tráfico broadcast o multicast elevado, comunicaciones recurrentes hacia múltiples destinos o puertos, o patrones que puedan afectar el rendimiento de la red. 11. La solución deberá permitir identificar protocolos y servicios comunes sobre TCP, UDP e ICMP, tales como HTTP, HTTPS, DNS, SMTP, POP3, IMAP, SIP, RTP u otros, según la información disponible en los flujos y capacidades de clasificación de la herramienta. 12. La solución deberá permitir monitorear el ancho de banda de enlaces e interfaces, diferenciando la distribución del tráfico por aplicación, protocolo, origen, destino, puerto, conversación o criterio equivalente. 13. La solución deberá permitir generar información útil para la gestión de calidad de servicio, priorización de tráfico o análisis de clases de servicio, siempre que los equipos de red proporcionen la información requerida. 14. La solución deberá permitir definir políticas de retención de información de tráfico, procurando conservar información detallada por un periodo mínimo de treinta (30) días o conforme a la capacidad licenciada, almacenamiento disponible y mejores prácticas del fabricante. 15. La solución deberá permitir identificar tendencias de consumo de aplicaciones, protocolos, usuarios, direcciones IP o segmentos de

		red, con la finalidad de apoyar la planificación de capacidad y la implementación de políticas de priorización o control de tráfico. 16. La solución deberá permitir identificar tráfico sospechoso, no esperado o no clasificado, con la finalidad de apoyar el diagnóstico de saturación, degradación de servicio, consumo anómalo o posibles incidentes de seguridad. 17. La solución deberá permitir investigar eventos de tráfico inesperado que puedan generar lentitud, altos tiempos de respuesta, intermitencia o utilización excesiva del ancho de banda, diferenciando entre posibles fallas del enlace y consumo generado por aplicaciones o dispositivos internos. 18. La solución deberá permitir generar informes históricos y detallados sobre la utilización de enlaces LAN, WAN, Internet u otros enlaces críticos definidos por la Entidad. 19. La solución deberá soportar el monitoreo de tráfico en redes IPv4 y, de ser aplicable, IPv6. 20. La solución deberá permitir alertar sobre tráfico anómalo o no permitido en puertos, protocolos o patrones definidos por la Entidad, siempre que dicha información pueda ser obtenida desde los equipos monitoreados o las fuentes de flujo disponibles. **<u>REPORTES Y ALERTAS</u>** 1. La plataforma deberá permitir la generación de reportes técnicos, operativos, ejecutivos y de análisis de tendencias sobre disponibilidad, rendimiento, capacidad, tráfico, alertas, eventos y estado general de la infraestructura monitoreada. 2. La solución deberá permitir generar reportes y gráficos sobre métricas de CPU, memoria, disco, interfaces, disponibilidad, actividad de servicios, eventos, alertas, desempeño de aplicaciones, accesos, errores o métricas equivalentes disponibles según el tipo de dispositivo o servicio monitoreado. 3. La solución deberá permitir reportes de tendencia, capacidad o proyección de crecimiento respecto de recursos monitoreados, tales como almacenamiento, disco, interfaces, consumo de ancho de banda, CPU, memoria u otros indicadores históricos disponibles. 4. Los reportes deberán poder exportarse, como mínimo, a formatos PDF, CSV, Excel o formatos equivalentes compatibles para análisis posterior. 5. La solución deberá permitir la generación automática y programada de reportes, así como su envío por correo electrónico a destinatarios definidos por la Entidad. 6. La solución deberá permitir configurar alertas adaptables y automatizadas, con mecanismos para reducir falsas alarmas, tales como dependencias, ventanas de mantenimiento, tiempos de espera, confirmación de eventos, severidades o reglas de correlación. 7. La solución deberá permitir recibir alertas en tiempo cercano al real cuando se detecten cambios relevantes en la disponibilidad, rendimiento, estado o configuración de los componentes monitoreados, siempre que dicha información sea proporcionada por el dispositivo o servicio correspondiente. 8. La solución deberá contar con alertas predefinidas y configurables, basadas en buenas prácticas de monitoreo de red, servidores, servicios, aplicaciones y enlaces críticos. 9. La solución deberá permitir notificaciones mediante correo electrónico y, opcionalmente, mediante otros mecanismos como SMS, aplicaciones móviles, webhooks, mensajería, integración con mesa de ayuda o APIs, según las capacidades de la herramienta. 10. La solución deberá permitir definir niveles de severidad, responsables, reglas de escalamiento, horarios de notificación y ventanas de mantenimiento para la adecuada gestión de alertas.
	PRESENTACIÓN-EMBALAJE (CAJA, ROLLO, BLÍSTER, FRASCO, ETC.)	NO CORRESPONDE
	INCLUYE IMAGEN REFERENCIAL (FOTO, VIDEO)-DE SER EL CASO.	NO CORRESPONDE
	PRUEBAS (TENER EN CUENTA QUE EL COSTO DE REQUERIR UNA MUESTRA PODRÍA DISTORSIONAR EL PRECIO DEL PRODUCTO A ADQUIRIR)	NO CORRESPONDE

5.	**LUGAR, PLAZO DE ENTREGA DE BIENES**	
	DIRECCIÓN EXACTA DE ENTREGA DE LOS BIENES	Sede Principal del OTASS, sito en Calle German Schreiber 210 - San Isidro
	ENTREGABLES	1. **LICENCIAMIENTO**: Documento del fabricante o distribuidor autorizado por el mismo, que acredite titularidad, cantidad, productos, módulos, fecha de inicio, fecha de fin, nivel de soporte y registro a

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

		nombre del OTASS. Las licencias deben estar asociadas a la cuenta de correo electrónico licencias@otass.gob.pe. El documento será remitido por el proveedor a través de la Mesa de Partes Virtual de OTASS, dirigido a la Unidad de Tecnologías de la Información. 2. **ACTA DE IMPLEMENTACIÓN**: Al finalizar la implementación del software y realizada la verificación de las funcionalidades de la misma, se firmará un Acta de Implementación. Dicha acta debe ser firmada por el proveedor y el jefe de la UTI. 3. **INFORME TÉCNICO DE IMPLEMENTACIÓN**: El proveedor deberá elaborar un informe técnico de las actividades realizadas para la instalación y configuración de la solución. Dicho informe deberá constar, como mínimo, de la siguiente documentación: • Carta de garantía comercial y soporte del fabricante, representante, distribuidor autorizado, según corresponda. • Carta de garantía y soporte del proveedor. • Procedimiento de atención de incidentes y requerimientos, incluyendo canales de atención, horarios, tiempos de respuesta y mecanismo de escalamiento. • Manual de administración, operación o guía técnica de uso de la plataforma de monitoreo implementada en la Entidad. • Informe de instalación, configuración y puesta en operación de la solución. • Relación de componentes implementados, credenciales entregadas, roles configurados, dispositivos incorporados, sensores habilitados y reportes configurados, según corresponda 4. **CAPACITACIÓN:** Material, registro de asistencia, evaluación o evidencia de ejecución y certificados/constancias de capacitación realizada por el proveedor. Todos los entregables deben ser remitidos a través de la mesa de partes virtual del OTASS: https://mesapartesdigital.otass.gob.pe/inicio Todos los entregables deben ser presentados en los plazos establecidos.
	PLAZOS	1. **PLAZO DE VIGENCIA DEL LICENCIAMIENTO** La vigencia de la licencia del software será por un plazo de 365 días calendarios. 2. **PLAZO DE IMPLEMENTACIÓN Y FIRMA DE ACTA DE IMPLEMENTACIÓN** El plazo de implementación de la solución será de hasta (30) días calendarios contados a partir del día siguiente de notificada la Orden de Compra. Al finalizar la implementación se firmará la respectiva acta de implementación. 3. **PLAZO PARA LA CAPACITACIÓN** El plazo para la realización de la capacitación será de hasta cinco (05) días calendarios, contados desde el día siguiente de finalizada la implementación de la solución. 4. **PLAZO PARA PRESENTACIÓN DEL INFORME TÉCNICO DE IMPLEMENTACIÓN** El proveedor tendrá un plazo de cinco (05) días calendario para la presentación del informe técnico de implementación, contabilizados desde el día siguiente de la firma del acta de implementación.
	HORARIO DE ATENCION	Lunes a viernes de 8:30 a 17:30 horas

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

	REQUISITOS MÍNIMOS DEL/DE LA PROVEEDOR/A	
	REQUISITOS DEL/DE LA PROVEEDOR/A	• El proveedor deberá contar con su Registro Nacional de Proveedores (RNP) habilitado. • Debe estar habilitado para contratar con el Estado. • Contar con RUC vigente y habilitado. • Ser fabricante, representante, distribuidor, partner, canal autorizado o contar con autorización válida para la comercialización de la solución de software de monitoreo ofertada. • Garantizar que la solución ofertada sea original, licenciada y cuente con el derecho de uso, soporte y actualizaciones. • Se aceptarán soluciones comerciales, propietarias, de código abierto empresarial u Open Source Enterprise, siempre que cuenten con soporte técnico formal, derecho de uso válido, documentación técnica, actualizaciones, parches, garantía comercial y respaldo del fabricante, titular de la solución, representante autorizado, partner o proveedor especializado durante la vigencia contratada. • Para las actividades de instalación, implementación, configuración, soporte o asistencia técnica, el proveedor deberá contar con personal técnico con experiencia o capacitación acreditada en la solución ofertada, o en soluciones de monitoreo de infraestructura tecnológica similares.
6.	EXPERIENCIA: MONTO FACTURADO (DE SER EL CASO)	El proveedor deberá acreditar un monto facturado acumulado equivalente a S/ 60,000.00 (sesenta mil con 00/100 soles), por la venta, suscripción, licenciamiento, implementación, soporte o mantenimiento de soluciones iguales o similares al objeto de la contratación, durante los ocho (8) años anteriores a la fecha de presentación de ofertas. Se consideran prestaciones similares, entre otras, las siguientes: • Venta, suscripción o licenciamiento de software de monitoreo de red. • Venta, suscripción o licenciamiento de software de monitoreo de infraestructura tecnológica. • Implementación, configuración, soporte o mantenimiento de plataformas de monitoreo de red, servidores, servicios, aplicaciones, enlaces de comunicaciones o equipos críticos de comunicaciones. • Soluciones de monitoreo de disponibilidad, rendimiento, tráfico, alertas, reportes, gestión de eventos o supervisión centralizada de infraestructura tecnológica. • Implementación, administración, soporte o mantenimiento de soluciones de infraestructura tecnológica para centros de datos, servidores, redes, VPN, servicios de hosting dedicado, plataformas de respaldo y seguridad, antivirus, EDR, continuidad operativa o servicios críticos de TI, siempre que guarden relación con la operación, disponibilidad, supervisión, administración o soporte de infraestructura tecnológica empresarial o institucional. La experiencia podrá acreditarse mediante copia simple de contratos, órdenes de compra, órdenes de servicio, conformidades, constancias de prestación, comprobantes de pago u otros documentos válidos que permitan verificar el objeto de la prestación, el monto facturado y la fecha correspondiente.
	REQUIERE PERSONAL ESPECIALIZADO (EN CASO LA NATURALEZA DE LA ADQUISICON LO REQUIERA)	Para la instalación, implementación, configuración, puesta en operación y/o asistencia técnica de la solución de software de monitoreo de red, el proveedor deberá contar, como mínimo, con el siguiente personal especializado: **<u>Un (01) Especialista</u>** • Titulado o bachiller o técnico egresado en carreras vinculadas a tecnologías de la información, sistemas, informática, computación, electrónica, telecomunicaciones, redes y comunicaciones o afines. • Contar con capacitación, curso, certificación o acreditación técnica relacionada con la solución ofertada o con soluciones de monitoreo de red, infraestructura tecnológica, servidores, aplicaciones, servicios o plataformas similares. • Acreditar experiencia mínima de tres (03) años en instalación, implementación, configuración, administración, soporte, mantenimiento o puesta en operación de soluciones de monitoreo de red, monitoreo de infraestructura tecnológica, servidores, aplicaciones, enlaces de comunicaciones, equipos de red o servicios tecnológicos similares.

Firmado digitalmente por
MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

7.	**ÁREA USUARIA / TÉCNICA QUE OTORGA LA CONFORMIDAD Y FORMA DE PAGO**			
	ÁREA QUE OTORGA LA CONFORMIDAD	La conformidad será otorgada por la Unidad de Tecnologías de la Información (UTI) a través del Acta de Conformidad correspondiente, previa revisión del entregable y habiendo verificado el cumplimiento de las especificaciones técnicas.		
	FORMA DE PAGO	Pago Único	TOTAL DE PAGOS	01
	OTASS cancela dentro de los diez (10) días siguientes a otorgada la conformidad final por parte de la Unidad indicada, salvo que existan supuestos no contemplados que ameriten mayor tiempo al indicado, aspecto que la OTASS puede indicar al contratista de considerarlo conveniente.			

8.	**PENALIDADES A APLICAR:**			
	TIPO DE PENALIDAD A APLICAR	<<Por mora en la ejecución>>		
	FORMA DE CÁLCULO	*Penalidad diaria = 0.10 x monto / F x plazo en días*	MONTO MÁXIMO APLICABLE	10% del monto total de la contratación
	PENALIDADES ADICIONALES	*<<Detalle si aplica otras penalidades diferentes a la entrega o a la indicada en el cuadro inicial>>*		

9.	**CONDICIONES COMPLEMENTARIAS**	
	EMBALAJE, ROTULACIÓN O ETIQUETADO. TRANSPORTE	
	ACONDICIONAMIENTO, MONTAJE E INSTALACIÓN	**CONSOLA CENTRALIZADA DE ADMINISTRACIÓN, MONITOREO Y GESTIÓN DE EVENTOS** La solución deberá contar con una consola centralizada de administración y monitoreo que permita gestionar, visualizar, supervisar y reportar el estado de la infraestructura tecnológica de la Entidad, incluyendo equipos de comunicaciones, servidores, servicios, aplicaciones y demás componentes críticos definidos por el OTASS. La herramienta deberá contar, de manera nativa o mediante componentes, módulos, integraciones soportadas, funcionalidades complementarias o mecanismos equivalentes incluidos en la oferta, con capacidades para monitorear, recolectar o analizar información mediante protocolos y tecnologías estándares, tales como: • SNMP v1/v2c/v3. • ICMP. • WMI, WinRM, SSH, API, agentes o mecanismos equivalentes, según corresponda. • Recepción de traps SNMP. • Recepción, almacenamiento y consulta de eventos Syslog. • NetFlow v5/v9, sFlow, J-Flow, IPFIX u otros protocolos equivalentes de análisis de tráfico. • Monitoreo de tráfico, ancho de banda, disponibilidad, latencia, pérdida de paquetes y estado de interfaces. • Monitoreo de calidad de servicio — QoS, incluyendo, de ser aplicable, tráfico de voz y video sobre IP. • Soporte para redes IPv4 y, de corresponder, IPv6. • Monitoreo de bases de datos, servicios, aplicaciones y procesos, según la compatibilidad de la herramienta. • Monitoreo de servicios o protocolos comunes, tales como HTTP, HTTPS, DNS, SMTP, POP3, IMAP, LDAP u otros equivalentes. • Monitoreo de certificados digitales SSL/TLS o equivalentes, de acuerdo con las capacidades de la solución. • Monitoreo de ambientes virtualizados, incluyendo plataformas como VMware ESXi/vCenter, Hyper-V u otras tecnologías equivalentes compatibles. La solución deberá permitir el monitoreo de dispositivos ubicados en sedes remotas o redes distintas a la red local principal, mediante mecanismos seguros de comunicación, tales como sondas, colectores, agentes, proxies, enlaces WAN, VPN, túneles cifrados, comunicación SSL/TLS u otros mecanismos equivalentes, de acuerdo con la arquitectura propuesta por el fabricante. La solución podrá emplear agentes, proxies, sondas, colectores o componentes equivalentes para el monitoreo de servidores, aplicaciones, servicios, sedes remotas o redes distribuidas, siempre que dichos componentes formen parte de la arquitectura soportada por la solución ofertada y se

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

		encuentren incluidos dentro de la propuesta económica. La herramienta deberá contar con funcionalidades para la elaboración de mapas, diagramas, dashboards o vistas gráficas personalizadas, que permitan representar la infraestructura monitoreada de acuerdo con las necesidades operativas de la Entidad. La herramienta deberá permitir, como mínimo, las siguientes funciones: • Monitoreo de periodos de actividad, inactividad, disponibilidad e indisponibilidad. • Monitoreo de disponibilidad, rendimiento, capacidad, tráfico y estado de dispositivos. • Monitoreo de QoS o métricas asociadas a calidad de servicio, cuando los dispositivos proporcionen dicha información. • Importación o uso de archivos MIB para ampliar el monitoreo SNMP de dispositivos compatibles. • Registro y consulta de eventos generados por la plataforma y por los dispositivos monitoreados. • Soporte para monitoreo en redes IPv4 y, de ser aplicable, IPv6. • Despliegue de sondas, colectores o componentes equivalentes para sedes remotas, cuando la arquitectura de la solución lo requiera. Dichos componentes deberán estar considerados dentro de la oferta económica, sin generar costos adicionales para cubrir el alcance mínimo requerido por la Entidad. • Generación de reportes personalizados respecto de los servicios, dispositivos, enlaces, aplicaciones y métricas monitoreadas. • Configuración de alertas, umbrales, notificaciones, ventanas de mantenimiento y reglas de escalamiento. • Visualización del estado general de la infraestructura mediante paneles o dashboards configurables. • Exportación de reportes en formatos de uso común, tales como PDF, CSV, XLSX o equivalentes. El proveedor deberá brindar asistencia técnica por fallas, incidencias o consultas asociadas al software de monitoreo, así como acceso a actualizaciones, parches, mejoras, documentación técnica y soporte durante el periodo licenciado, conforme a las condiciones establecidas por el fabricante. La solución ofertada deberá contar con licenciamiento original, válido y registrado a nombre del OTASS, incluyendo el derecho de uso, soporte, actualizaciones y garantía comercial correspondiente durante la vigencia contratada.
	CAPACITACIÓN Y/O ENTRENAMIENTO	El proveedor deberá brindar capacitación y/o entrenamiento a dos (02) profesionales y/o técnicos de la Unidad de Tecnologías de la Información del OTASS, respecto del uso, administración, configuración, operación y monitoreo de la solución de software implementada. La capacitación podrá realizarse en modalidad virtual, presencial o mixta, según coordinación con el OTASS. La duración mínima de la capacitación será de cuatro (04) horas efectivas y deberá comprender, como mínimo, los siguientes temas: • Acceso y navegación en la consola de administración. • Administración de usuarios, roles o perfiles. • Configuración de dispositivos, sensores, monitores o elementos equivalentes. • Creación y administración de grupos, vistas, mapas o dashboards. • Configuración de umbrales, alertas, notificaciones y ventanas de mantenimiento. • Generación, programación y exportación de reportes. • Revisión de eventos, logs, incidencias y estado de los componentes monitoreados. • Buenas prácticas para la operación, administración y mantenimiento de la plataforma. Al término de la capacitación, el proveedor deberá entregar la presentación, material utilizado, manuales, guías rápidas o documentación técnica correspondiente, así como la constancia de capacitación o documento equivalente que acredite la participación del personal designado por la Entidad.

	ACCESORIOS COMPLEMENTARIOS	NO CORRESPONDE
	MANTENIMIENTO PREVENTIVO	En caso el fabricante y/o el proveedor programe actividades de mantenimiento preventivo, actualización, parcheo, mejora, reinicio de servicios o intervención técnica sobre la solución de monitoreo que pudieran generar indisponibilidad, degradación del servicio o afectación temporal de la operación, deberá comunicarlo previamente a la Entidad. La comunicación deberá realizarse con una anticipación mínima de cuarenta y ocho (48) horas, mediante correo electrónico dirigido al personal designado por el OTASS, indicando como mínimo: • Fecha y hora de inicio del mantenimiento. • Duración estimada. • Alcance de la actividad. • Componentes o servicios que podrían verse afectados. • Riesgo de indisponibilidad o degradación. • Medidas de contingencia o reversión, de corresponder. • Personal responsable de la atención. Las actividades de mantenimiento que impliquen interrupción del servicio deberán ser coordinadas y aprobadas previamente por la Entidad, procurando que se ejecuten en horarios de menor impacto operativo.
	SOPORTE TÉCNICO	El proveedor deberá brindar soporte técnico durante la vigencia del licenciamiento, para la atención de incidentes, fallas, errores, consultas técnicas, problemas de acceso, degradación del servicio, actualización, operación o configuración de la solución de monitoreo implementada. El soporte técnico deberá prestarse como mínimo mediante correo electrónico, teléfono, mesa de ayuda, portal web u otro canal formal de atención informado por el proveedor. Para incidentes críticos que afecten la disponibilidad u operación principal de la plataforma de monitoreo, el proveedor deberá garantizar atención en modalidad 24x7x365, con un tiempo máximo de respuesta inicial de dos (02) horas, contado desde el registro o comunicación del incidente por parte de la Entidad. El proveedor deberá contar con la capacidad de escalar los incidentes al fabricante, mayorista, representante o centro de soporte especializado de la solución ofertada, cuando la naturaleza del incidente lo requiera o cuando no pueda ser resuelto en el primer nivel de atención. Como parte de la oferta o durante la suscripción del contrato, el proveedor deberá presentar una carta de compromiso de soporte técnico, indicando los canales de atención, horario de atención, niveles de severidad, tiempos de respuesta, procedimiento de escalamiento y responsables de la atención. El soporte deberá incluir, como mínimo: • Atención de incidentes asociados al funcionamiento de la solución. • Asistencia técnica sobre configuración y operación de la plataforma. • Soporte ante errores, fallas o indisponibilidad del software. • Orientación para la aplicación de parches, actualizaciones o mejoras. • Escalamiento al fabricante o soporte especializado, cuando corresponda. • Seguimiento hasta el cierre del incidente o requerimiento.
	MUESTRAS (De acuerdo a la naturaleza de los bienes, se pueden requerir la presentación de muestra para la evaluación y verificación del cumplimiento de la especificación técnica).	NO CORRESPONDE
	GARANTIA COMERCIAL	La solución ofertada deberá contar con una garantía comercial por un periodo no menor de trescientos sesenta y cinco (365) días calendario, contados a partir del día siguiente

Firmado digitalmente por
MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

		de la conformidad de la implementación, activación, configuración y puesta en operación de la solución de monitoreo. **1. Garantía, soporte y actualizaciones del fabricante** La garantía del fabricante, o del titular de la solución ofertada, deberá permitir a la Entidad acceder durante la vigencia contratada, como mínimo, a lo siguiente: • Derecho de uso de la solución licenciada o suscrita. • Soporte técnico del fabricante, representante, mayorista o canal autorizado, según corresponda. • Acceso a parches, actualizaciones, correcciones y mejoras del software. • Actualizaciones de seguridad, alertas técnicas y versiones de mantenimiento. • Actualización de documentación técnica, guías, manuales o base de conocimiento disponible. • Acceso a nuevas versiones, versiones menores o versiones principales, de acuerdo con las condiciones comerciales y políticas de licenciamiento del fabricante. • Atención o escalamiento de incidentes críticos relacionados con fallas de funcionamiento de la solución. Para incidentes críticos que afecten la disponibilidad u operación principal de la plataforma de monitoreo, el soporte deberá contemplar atención 24x7x365, con un tiempo máximo de respuesta inicial de dos (02) horas, siempre que dicha condición forme parte del esquema de soporte ofertado y se encuentre debidamente acreditada por el fabricante, representante autorizado o proveedor. **2. Garantía y soporte del/de la proveedor/a** El proveedor deberá garantizar el correcto funcionamiento de la solución de monitoreo implementada durante un periodo mínimo de trescientos sesenta y cinco (365) días calendario, contados a partir del día siguiente de la conformidad de la implementación y puesta en operación. Dicha garantía deberá cubrir, como mínimo: • Fallas de instalación, configuración o puesta en operación atribuibles al proveedor. • Incidentes de funcionamiento de la solución implementada. • Problemas de compatibilidad identificados durante la operación, siempre que estén relacionados con los componentes, versiones o configuración ofertada. • Asistencia técnica para la corrección de errores, ajustes de configuración o restablecimiento de funcionalidades. • Coordinación y escalamiento ante el fabricante, representante, mayorista o centro de soporte especializado, cuando corresponda. • Acompañamiento técnico hasta la atención, solución o cierre del incidente reportado por la Entidad. El proveedor deberá presentar una carta de garantía comercial y soporte, indicando el periodo de cobertura, canales de atención, procedimiento de reporte de incidentes, niveles de severidad, tiempos de respuesta y mecanismo de escalamiento.

10.	**OTRAS OBLIGACIONES DE PARTE DEL/DE LA PROVEEDOR/A**	
	SEGUROS APLICABLES	NO CORRESPONDE
	CONFIDENCIALIDAD	El proveedor se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita por el OTASS, toda la información que le sea suministrada y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del contrato. El proveedor del servicio debe mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida de revelarlo a terceros. Dicha obligación comprende que la información que sea entregada, como también la que se genere durante las realizaciones de actividades previas a la ejecución del contrato, durante su ejecución y la

		producida una vez que haya concluido el contrato. Asimismo, aun cuando sea índole publica, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el proveedor para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del OTASS.
	PROPIEDAD INTELECTUAL	NO CORRESPONDE
	DERECHOS PARA EL USO DE IMAGEN PERSONAL	NO CORRESPONDE
	COMPROMISO DE CUMPLIR Y OBSERVAR LO ESTABLECIDO EN LA LEY DE SEGURIDAD Y SALUD EN EL TRABAJO (APROBADO MEDIANTE LEY N° 29783) Y EN SU REGLAMENTO (APROBADO MEDIANTE DECRETO SUPREMO Nº 005-2012-TR)	
	OTRAS CONDICIONES CONTRACTUALES IMPORTANTES	NO CORRESPONDE
11.	**SISTEMA DE GESTION ANTISOBORNO**	
	"EL/LA PROVEEDOR/A SE OBLIGA A CONDUCIRSE EN TODO MOMENTO, DURANTE LA EJECUCIÓN DEL CONTRATO, CON HONESTIDAD, PROBIDAD, VERACIDAD E INTEGRIDAD Y DE NO COMETER ACTOS ILEGALES O DE CORRUPCIÓN, DIRECTA O INDIRECTAMENTE O A TRAVÉS DE SUS SOCIOS, ACCIONISTAS, PARTICIPACIONISTAS, INTEGRANTES DE LOS ÓRGANOS DE ADMINISTRACIÓN, APODERADOS, REPRESENTANTES LEGALES, GERENTES, DIRECTORES, ASESORES Y PERSONAS VINCULADAS A LAS QUE SE REFIERE EL ARTÍCULO 7 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO".	
12.	**CLAUSULA: GARANTIA**	
	DE CORRESPONDER, DE CONFORMIDAD CON EL ARTÍCULO 61 DE LA LEY N° 32069 LEY GENERAL DE CONTRATACIONES PÚBLICAS.	
13	**CLAUSULA: ANTICORRUPCIÓN Y ANTISOBORNO**	
	EL PROVEEDOR DECLARA Y GARANTIZA NO HABER OFRECIDO, NEGOCIADO, PROMETIDO O EFECTUADO NINGÚN PAGO O ENTREGA DE CUALQUIER BENEFICIO O INCENTIVO ILEGAL, DE MANERA DIRECTA O INDIRECTA, A LOS EVALUADORES DEL PROCESO DE CONTRATACIÓN O CUALQUIER SERVIDOR DE LA ENTIDAD CONTRATANTE. ASIMISMO, EL PROVEEDOR SE OBLIGA A MANTENER UNA CONDUCTA PROBA E ÍNTEGRA DURANTE LA VIGENCIA DEL CONTRATO/ORDEN DE SERVICIO U COMPRA, Y DESPUÉS DE CULMINADO EL MISMO EN CASO EXISTAN CONTROVERSIAS PENDIENTES DE RESOLVER, LO QUE SUPONE ACTUAR CON PROBIDAD, SIN COMETER ACTOS ILÍCITOS, DIRECTA O INDIRECTAMENTE. AUNADO A ELLO, EL PROVEEDOR SE OBLIGA A ABSTENERSE DE OFRECER, NEGOCIAR, PROMETER O DAR REGALOS, CORTESÍAS, INVITACIONES, DONATIVOS O CUALQUIER BENEFICIO O INCENTIVO ILEGAL, DIRECTA O INDIRECTAMENTE, A FUNCIONARIOS PÚBLICOS, SERVIDORES PÚBLICOS, LOCADORES DE SERVICIOS O PROVEEDORES DE SERVICIOS DEL ÁREA USUARIA, DE LA DEPENDENCIA ENCARGADA DE LA CONTRATACIÓN, ACTORES DEL PROCESO DE CONTRATACIÓN Y/O CUALQUIER SERVIDOR DE LA ENTIDAD CONTRATANTE, CON LA FINALIDAD DE OBTENER ALGUNA VENTAJA INDEBIDA O BENEFICIO ILÍCITO. EN ESA LÍNEA, SE OBLIGA A ADOPTAR LAS MEDIDAS TÉCNICAS, ORGANIZATIVAS Y/O DE PERSONAL NECESARIAS PARA ASEGURAR QUE NO SE PRACTIQUEN LOS ACTOS PREVIAMENTE SEÑALADOS. ADICIONALMENTE, EL PROVEEDOR SE COMPROMETE A DENUNCIAR OPORTUNAMENTE ANTE LAS AUTORIDADES COMPETENTES LOS ACTOS DE CORRUPCIÓN O DE INCONDUCTA FUNCIONAL DE LOS CUALES TUVIERA CONOCIMIENTO DURANTE LA EJECUCIÓN DEL CONTRATO/ORDEN DE SERVICIO U COMPRA CON LA ENTIDAD CONTRATANTE.	
14	**CLAUSULA: SOLUCIÓN DE CONTROVERSIAS**	
	TODAS LAS CONTROVERSIAS QUE SURJAN ENTRE LAS PARTES SOBRE LA VALIDEZ, NULIDAD, INTERPRETACIÓN, EJECUCIÓN, TERMINACIÓN O EFICACIA DE LOS CONTRATOS MENORES SE RESUELVEN MEDIANTE CONCILIACIÓN, CONFORME LO DISPUESTO EN EL NUMERAL 81.3 DEL ARTÍCULO 81 DE LA LEY N° 32069 LEY GENERAL DE CONTRATACIONES PÚBLICAS.	
15	**CLAUSULA DE RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO**	
	CUALQUIERA DE LAS PARTES PUEDE RESOLVER EL CONTRATO, DE CONFORMIDAD CON EL NUMERAL 68.1 DEL ARTÍCULO 68 DE LA LEY N° 32069, LEY GENERAL DE CONTRATACIONES PÚBLICAS. DE ENCONTRARSE EN ALGUNO DE LOS SUPUESTOS DE RESOLUCIÓN DEL CONTRATO, LAS PARTES PROCEDEN DE ACUERDO A LO ESTABLECIDO EN EL ARTÍCULO 122 DEL REGLAMENTO DE LA LEY N° 32069, LEY GENERAL DE CONTRATACIONES PÚBLICAS, APROBADO POR DECRETO SUPREMO N° 009-2025-EF. ASIMISMO, SON CAUSALES DE RESOLUCIÓN DE CONTRATO LA PRESENTACIÓN CON INFORMACIÓN INEXACTA O FALSA DE LA DECLARACIÓN JURADA DE PROHIBICIONES E INCOMPATIBILIDADES A QUE SE HACE REFERENCIA EN LA LEY DE PREVENCIÓN Y MITIGACIÓN DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PÚBLICO LEY N° 31564. , EN CASO SE INCUMPLA CON LOS IMPEDIMENTOS SEÑALADOS EN EL ARTÍCULO 5 DE DICHA LEY SE APLICARÁ LA INHABILITACIÓN POR CINCO AÑOS PARA CONTRATAR O PRESTAR SERVICIOS AL ESTADO, BAJO CUALQUIER MODALIDAD (DE CORRESPONDER).	
16	**CLAUSULA: GESTIÓN DE RIESGOS.**	
	LAS PARTES REALIZAN LA GESTIÓN DE RIESGOS DE ACUERDO CON LO ESTABLECIDO EN EL PRESENTE CONTRATO/ORDEN DE SERVICIO U COMPRA Y LOS DOCUMENTOS QUE LO CONFORMAN,	

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500

	A FIN DE TOMAR DECISIONES INFORMADAS, APROVECHANDO EL IMPACTO DE RIESGOS POSITIVOS Y DISMINUYENDO LA PROBABILIDAD DE LOS RIESGOS NEGATIVOS Y SU IMPACTO DURANTE LA EJECUCIÓN CONTRACTUAL, CONSIDERANDO LA FINALIDAD PÚBLICA DE LA CONTRATACIÓN.

17.	**APROBADOR DEL REQUERIMIENTO**	
	FIRMA DEL APROBADOR DEL REQUERIMIENTO	
	LUGAR Y FECHA	SAN ISIDRO, 15 DE JULIO DE 2026

Firmado digitalmente por
MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 18:41:09-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/16 09:27:06-0500