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 LICENCIAS DE SOFTWARE DE SEGURIDAD DE ENDPOINT (ANTIVIRUS) PARA EL OTASS		
	ACTIVIDAD DEL POI	AOI00158900145: ELABORACIÓN DE INFORMES DE OPERATIVIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA		
	META	090		
	FINALIDAD PUBLICA	Fortalecer la seguridad digital, continuidad operativa y protección de la información institucional mediante la prevención, detección, investigación y respuesta frente a malware, ransomware, ataques sin archivos, explotación de vulnerabilidades, abuso de herramientas legítimas y otras amenazas que afecten las estaciones de trabajo, equipos portátiles y servidores del OTASS.		
	OBJETO DE LA CONTRATACIÓN	Contar con una plataforma empresarial de seguridad de endpoint, administrada centralizadamente, que proporcione protección preventiva y capacidades EDR, permita aplicar políticas de seguridad, responder remotamente ante incidentes, generar evidencias y reportes, y operar dentro de la infraestructura tecnológica de la Entidad.		
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	Licencias para estaciones de trabajo y portátiles: **450** Licencias para servidores Windows: **70** Licencias para servidores Linux: **25**
	UNIDAD DE MEDIDA (UNIDAD, CIENTOS, GALÓN, ETC.)	Unidad

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

	DIMENSIONES ((TAMAÑO, PESO, VOLUMEN, ETC.)	NO CORRESPONDE
	CAPACIDAD (TENSIÓN, CORRIENTE, POTENCIA, RENDIMIENTO, VELOCIDAD, ETC.), EN CASO CORRESPONDA.	**1. LICENCIAMIENTO Y REGISTRO** 1.1. Las licencias deberán ser nuevas, originales, vigentes y proporcionadas por el fabricante o por un canal autorizado. 1.2. Las licencias deberán registrarse a nombre del OTASS. La cuenta de registro será licencias@otass.gob.pe. 1.3. El licenciamiento deberá cubrir la cantidad de endpoints y servidores indicada en la sección de cantidades, incluyendo las capacidades obligatorias EPP/EDR y su administración centralizada. 1.4. Las licencias deberán poder reasignarse cuando un equipo sea reemplazado, dado de baja, reinstalado o transferido, de acuerdo con las condiciones del fabricante y sin pérdida del saldo de vigencia. 1.5. El postor deberá identificar expresamente cada producto, edición, módulo, complemento y nivel de soporte ofertado. No se aceptará acreditar una función mediante un módulo que no haya sido cotizado. **2. COMPATIBILIDAD CON SISTEMAS OPERATIVOS** 2.1. La solución deberá proteger versiones de Windows 10 y Windows 11, en arquitecturas de 64 bits. El postor presentará la matriz oficial de compatibilidad vigente. 2.2. La solución deberá proteger Windows Server 2016 o superior. El postor deberá indicar restricciones, soporte extendido o medidas compensatorias para versiones legadas de sistemas operativos de servidor de Microsoft. 2.3. La solución deberá disponer de protección para servidores Linux empresariales. El postor detallará distribuciones, versiones, kernel, arquitecturas y diferencias funcionales respecto de Windows. 2.4. Se aceptará que determinadas capacidades de control de dispositivos, firewall, cifrado, rollback o respuesta varíen por sistema operativo, siempre que las capacidades esenciales de antimalware, protección conductual, EDR, aislamiento o contención y administración central estén disponibles para las plataformas solicitadas, o se declare claramente la equivalencia aplicable. 2.5. El postor deberá indicar los requerimientos de CPU, memoria, almacenamiento, conectividad, exclusiones y compatibilidad con virtualización, VDI y aplicaciones críticas. **3. CONSOLA CENTRAL DE ADMINISTRACIÓN** 3.1. La solución deberá contar con una consola central web o aplicación administrativa soportada, accesible mediante protocolo seguro y capaz de gestionar políticas, dispositivos, alertas, incidentes, actualizaciones y licencias. 3.2. La interfaz deberá estar disponible en español o, en su defecto, el fabricante deberá proporcionar documentación y soporte en español. 3.3. La consola deberá permitir organizar equipos por grupos, etiquetas, unidades organizativas, tipo de sistema operativo, ubicación u otros criterios equivalentes, y asignar políticas diferenciadas. 3.4. Deberá incluir control de acceso basado en roles y permitir perfiles de solo lectura, operación, investigación y administración, o roles equivalentes. 3.5. Deberá soportar autenticación multifactor para administradores, directamente o mediante integración con un proveedor de identidad compatible. 3.6. Deberá registrar acciones administrativas y cambios de políticas mediante bitácora de auditoría consultable y exportable. 3.7. Deberá mostrar el estado de protección, última comunicación, versión del agente, sistema operativo,

		direcciones de red, políticas asignadas, alertas y estado de actualización de cada dispositivo. 3.8. La consola deberá permitir identificar equipos sin protección, desconectados, desactualizados, con errores o que no cumplen la política asignada. 3.9. Se aceptará consola en nube, local o híbrida. Para SaaS, el fabricante deberá informar el compromiso de disponibilidad, ubicación o región de procesamiento y mecanismos de continuidad. Para local, deberá indicar dimensionamiento, respaldo y recuperación. 3.10. La solución deberá permitir descargar o exportar configuraciones, inventarios, eventos y reportes, o contar con mecanismos equivalentes de respaldo y recuperación. **4. PROTECCIÓN PREVENTIVA EPP/NGAV** 4.1. La solución deberá detectar, bloquear, poner en cuarentena, eliminar o remediar virus, troyanos, gusanos, spyware, adware, rootkits, herramientas potencialmente no deseadas y otras formas de malware. 4.2. Deberá proteger frente a amenazas conocidas y desconocidas mediante una combinación de firmas, reputación, análisis heurístico, machine learning, análisis conductual, inteligencia en la nube, sandboxing o técnicas equivalentes. 4.3. Deberá detectar y bloquear ataques sin archivos, abuso de PowerShell, WMI, scripts, macros, herramientas de administración remota y binarios legítimos utilizados con fines maliciosos, mediante controles conductuales o equivalentes. 4.4. Deberá incluir protección contra ransomware que detecte comportamientos de cifrado o destrucción masiva, detenga procesos maliciosos y facilite la recuperación, reversión, remediación o preservación de archivos cuando la tecnología ofertada lo permita. 4.5. Deberá incluir prevención de exploits y técnicas de ataque a memoria, tales como desbordamientos de búfer, inyección de procesos, ROP, carga maliciosa de DLL, escalamiento de privilegios o mecanismos equivalentes. 4.6. Deberá analizar archivos en tiempo real al crear, abrir, ejecutar, copiar, descargar o modificar, y permitir análisis completos, rápidos, personalizados y programados. 4.7. Deberá consultar reputación de archivos, direcciones, dominios o indicadores en servicios del fabricante y mantener protección local razonable durante interrupciones temporales de internet. 4.8. Deberá proteger sus servicios, archivos, configuraciones y procesos contra deshabilitación, alteración o desinstalación no autorizada mediante protección antimanipulación, contraseña, token o mecanismo equivalente. 4.9. La solución deberá permitir exclusiones controladas por ruta, archivo, proceso, hash, certificado, aplicación, extensión o criterio equivalente, manteniendo trazabilidad de los cambios. 4.10. Deberá permitir enviar muestras sospechosas al fabricante o a un entorno de análisis, de manera manual o automática, respetando las políticas de privacidad y exclusión configuradas por la Entidad. **5. REDUCCIÓN DE SUPERFICIE DE ATAQUE Y CONTROLES DEL ENDPOINT** 5.1. La solución deberá incluir control de dispositivos o periféricos que permita, como mínimo, bloquear, permitir y establecer acceso de solo lectura para almacenamiento removible USB, con excepciones por dispositivo, identificador, grupo o criterio equivalente. 5.2. La solución deberá permitir bloquear o restringir aplicaciones, scripts o ejecutables mediante reglas, reputación, listas de permitidos/denegados, indicadores, hash, certificado, ruta o capacidades equivalentes.

		5.3. La solución deberá incluir firewall de endpoint o permitir la administración centralizada, integración o coexistencia documentada con el firewall nativo del sistema operativo, sin deshabilitar controles esenciales de red. 5.4. Deberá bloquear o advertir sobre sitios, dominios, URL o descargas maliciosas mediante reputación web, análisis de tráfico, protección de red, DNS, extensión de navegador o mecanismo equivalente. 5.5. Deberá permitir crear indicadores personalizados de bloqueo o alerta para, como mínimo, archivos, hashes, direcciones IP, dominios o URL, según las capacidades soportadas por la plataforma. 5.6. Opcionalmente, la solución deberá contar con capacidades de DLP, cifrado de disco, gestión de parches, NAC, filtrado web por categorías y simulación de phishing. **6. DETECCIÓN Y RESPUESTA DE ENDPOINT - EDR** 6.1. La solución deberá incluir capacidades EDR para recopilar y correlacionar telemetría relevante de procesos, archivos, conexiones, usuarios, eventos de seguridad y actividad del endpoint. 6.2. Deberá generar alertas e incidentes con información que facilite identificar el equipo, usuario, proceso, archivo, línea de tiempo, severidad, técnica de ataque o evidencias relacionadas. 6.3. Deberá permitir investigar amenazas mediante búsqueda, consultas, filtros, árbol de procesos, línea de tiempo, grafo, narrativa del ataque o mecanismos equivalentes. 6.4. Deberá permitir aislar o contener remotamente un endpoint comprometido, manteniendo comunicación con la plataforma de administración y servicios necesarios para su recuperación. 6.5. Deberá permitir ejecutar acciones de respuesta tales como finalizar procesos, eliminar o poner en cuarentena archivos, bloquear indicadores, iniciar análisis, recopilar información o acciones equivalentes. 6.6. Deberá contar con mecanismos de remediación automática, guiada o manual para reducir el tiempo de respuesta ante incidentes. 6.7. La telemetría o datos de investigación deberán conservarse por un mínimo de quince (15) días calendario. Se considerará favorable una retención incluida de treinta (30) días o más. 6.8. Deberá permitir exportar evidencias, incidentes, eventos o resultados de investigación en formatos de uso común o mediante API. 6.9. La solución deberá mapear detecciones a MITRE ATT&CK o a una taxonomía técnica equivalente que facilite comprender tácticas y técnicas utilizadas. **7. INSTALACIÓN, DESPLIEGUE, ACTUALIZACIÓN Y MIGRACIÓN** 7.1. La solución deberá permitir despliegue masivo mediante, al menos, dos mecanismos entre los siguientes: herramienta del fabricante, políticas de dominio, Microsoft Intune, Microsoft Configuration Manager, scripts, paquetes MSI/EXE/PKG/RPM/DEB, imagen maestra, enlace de instalación o herramienta equivalente. 7.2. Deberá permitir instalación manual y desatendida, así como la incorporación de equipos remotos a través de internet, cuando la modalidad de la solución lo soporte. 7.3. La coexistencia o remoción de una solución antivirus anterior deberá realizarse mediante herramienta del fabricante, procedimiento documentado, script del proveedor o utilidad autorizada. 7.4. La solución deberá actualizar automáticamente agentes, motores, modelos, firmas, reglas e inteligencia de amenazas. 7.5. Deberá permitir controlar la distribución de actualizaciones mediante ventanas, anillos, grupos piloto, relays, caché,

		pares, límites de ancho de banda o mecanismos equivalentes, según la arquitectura ofertada. 7.6. Las actualizaciones deberán ser firmadas, verificadas y distribuidas mediante canales seguros. El fabricante deberá contar con un procedimiento para retirar, detener o revertir actualizaciones defectuosas. **8. INTEGRACIÓN E INTEROPERABILIDAD** 8.1. La solución deberá integrarse con Active Directory, Microsoft Entra ID, LDAP, grupos de dispositivos, importación CSV o mecanismos equivalentes para organizar usuarios y equipos. 8.2. Deberá proporcionar API, syslog, webhook, conector SIEM, exportación programada o mecanismo equivalente para integrar alertas y eventos con herramientas de ciberseguridad o monitoreo de la Entidad. 8.3. La integración con Cisco ISE, FortiNAC, Aruba ClearPass, firewalls u otras plataformas NAC podrá presentarse como capacidad adicional, pero no constituye requisito obligatorio. 8.4. La solución deberá permitir exportar inventarios, alertas, incidentes y estado de protección, como mínimo en CSV, PDF, JSON, HTML o mediante API, según el tipo de información. **9. ALERTAS, REPORTES Y AUDITORÍA** 9.1. La plataforma deberá enviar notificaciones por correo electrónico y/o integraciones equivalentes ante eventos críticos, fallos de protección, infecciones, aislamiento, manipulación o incumplimiento de políticas. 9.2. Deberá proporcionar paneles y reportes del estado de protección, cobertura de agentes, versiones, amenazas, incidentes, equipos sin comunicación, actualizaciones y acciones de respuesta. 9.3. Los reportes deberán poder filtrarse por periodo, grupo, equipo, usuario, severidad, tipo de amenaza o criterio equivalente. 9.4. Deberá permitir exportación de reportes en PDF, CSV, HTML u otro formato de uso común. Se considerará favorable la programación y envío automático de reportes. 9.5. Deberá registrar eventos y acciones de administración suficientes para auditoría, incluyendo usuario, fecha, operación y objeto afectado. **10. SEGURIDAD, PRIVACIDAD Y CONTINUIDAD DEL SERVICIO** 10.1. La comunicación entre agentes, consola y servicios del fabricante deberá emplear cifrado y certificados vigentes conforme a prácticas de seguridad aceptadas. 10.2. La plataforma deberá permitir MFA y control de acceso por roles para cuentas administrativas, así como bitácora de cambios y accesos relevantes. 10.3. La solución deberá permitir configurar exclusiones para archivos, rutas o repositorios sensibles que no deban enviarse a análisis en la nube, sin deshabilitar la protección del resto del entorno. 10.4. El tratamiento de información deberá cumplir la normativa peruana aplicable en protección de datos personales, seguridad digital y confidencialidad, así como las políticas institucionales del OTASS. 10.5. El fabricante deberá publicar avisos de seguridad, versiones soportadas, ciclo de vida y procedimientos de actualización. El proveedor comunicará oportunamente vulnerabilidades críticas que afecten la solución. 10.6. En caso de consola SaaS, el proveedor deberá informar el compromiso de disponibilidad y soporte del fabricante.

		11. RENDIMIENTO Y OPERACIÓN 11.1. El agente deberá operar sin afectar la disponibilidad de las aplicaciones informáticas de la Entidad. El proveedor deberá declarar consumos típicos y requisitos mínimos. 11.2. La solución deberá permitir programar análisis, actualizaciones y tareas intensivas fuera de horarios de mayor demanda, o aplicar mecanismos automáticos de optimización. 11.3. El proveedor deberá configurar exclusiones recomendadas por los fabricantes de aplicaciones críticas, previa validación de la UTI y sin reducir innecesariamente la cobertura de seguridad. 11.4. La solución deberá mantener protección local esencial cuando el endpoint pierda temporalmente comunicación con la consola o internet, y sincronizar eventos al restablecerse la conectividad. **12. MÓDULOS Y CAPACIDADES OPCIONALES** 12.1. Prevención de pérdida de datos (DLP) basada en contenido, patrones, diccionarios, tipos de archivo y canales de salida. 12.2. Gestión de vulnerabilidades y administración de parches de sistema operativo y aplicaciones de terceros. 12.3. Cifrado de disco completo, archivos, carpetas o medios removibles. 12.4. Filtrado web por categorías de productividad, contenido adulto, apuestas, proxy, violencia u otras. 12.5. Simulación de phishing y capacitación de concientización, con biblioteca de plantillas personalizable, sin exigir una cantidad exacta. 12.6. MDR 24x7, threat hunting gestionado, retainer de respuesta a incidentes o SOC como servicio. 12.7. XDR con telemetría nativa de correo, identidad, red, nube, firewall u otras fuentes distintas al endpoint. 12.8. Integración o postura para NAC, Zero Trust Network Access o control de acceso basado en estado del endpoint. 12.9. Protección para dispositivos móviles, contenedores, cargas cloud, Kubernetes, IoT u OT.
	FORMA, COLOR, TEXTURAS.	NO CORRESPONDE
	MATERIAL (POR EJEMPLO: CUERO, TELA DE ALGODÓN, MADERA, METAL, FIERRO, MELANINE, ETC.).	NO CORRESPONDE
	ACCESORIOS PRINCIPALES	NO CORRESPONDE
	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	La entrega del bien se realizará en el Cuarto de Telecomunicaciones del OTASS, sito en el cuarto piso, Oficina 403, del edificio ubicado en la calle German Schreiber 210 - San Isidro. **ENTREGABLES** 1. **PLAN DE TRABAJO**: El proveedor deberá entregar un plan de trabajo para la implementación de la solución. El plan debe incluir arquitectura, inventario, requisitos, responsables, actividades, cronograma, piloto, migración, contingencia, despliegue, pruebas y criterios de aceptación.

		El plan de trabajo será revisado y aprobado vía correo electrónico por la UTI. Las actividades y cronograma del plan de trabajo deben ajustarse para que los equipos informáticos se encuentren protegidos con la nueva solución desde el 19 de noviembre de 2026. 2. **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 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. 3. **ACTA DE IMPLEMENTACIÓN**: Al finalizar la implementación de la solución 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. 4. **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: • Informe de actividades, equipos intervenidos, políticas configuradas, exclusiones, pruebas, incidencias y estado final. • Certificado y registro de las licencias de la solución a nombre del OTASS. • Acceso al portal del soporte del fabricante. • Procedimiento de atención de incidentes y requerimientos. • Manual de administración, procedimiento de instalación y retiro, recuperación, actualización, aislamiento, respuesta, respaldo/exportación y escalamiento. • Manual técnico de administración, gestión y/o operación de la consola de administración de la solución, el mismo que deberá describir todas sus funcionalidades. • Certificado del fabricante y garantía comercial. • Carta de garantía y soporte del proveedor. 5. **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	El plazo de la vigencia del software será por 365 días calendarios, los plazos para plan de trabajo e implementación se detallan a continuación: 1. **PLAZO DE VIGENCIA DEL LICENCIAMIENTO** La vigencia de la licencia de la solución será por un plazo de 365 días. La activación de las licencias debe realizarse el 19 de noviembre del 2026. 2. **PLAZO PARA LA PRESENTACIÓN PLAN DE TRABAJO** El proveedor deberá remitir el plan de trabajo como máximo a los tres (03) días calendarios posteriores a la notificación de la orden de compra.

Firmado digitalmente por
MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

		3. PLAZO DE IMPLEMENTACIÓN Y FIRMA DE ACTA DE IMPLEMENTACIÓN El plazo de implementación de la solución será de hasta (30) días calendarios previos al periodo de inicio de la vigencia del licenciamiento. Al finalizar la implementación se firmará la respectiva acta de implementación. **4. PLAZO PARA LA CAPACITACIÓN** El plazo para la realización de la capacitación será de hasta siete (07) días calendarios, contados desde el día siguiente de finalizada la implementación de la solución. **5. 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 desde las 8.30 a.m. a 5.30 p.m.

6.	**REQUISITOS MÍNIMOS DEL/DE LA PROVEEDOR/A**	
	REQUISITOS DEL/DE LA PROVEEDOR/A	• Contar con inscripción vigente en el Registro Nacional de Proveedores (RNP). • Contar con Registro Único de Contribuyentes (RUC) activo y habido. • No encontrarse impedido, suspendido ni inhabilitado para contratar con el Estado. • Carta emitida por el fabricante. • Certificado de distribuidor, reseller, partner o canal autorizado. • Constancia de registro en el programa de socios del fabricante. • Carta emitida por un mayorista o distribuidor autorizado en el territorio nacional. • Otro documento oficial que permita verificar la autorización para comercializar o implementar la solución ofertada.

	EXPERIENCIA: MONTO FACTURADO (DE SER EL CASO)	• El proveedor deberá acreditar un monto facturado acumulado mínimo de S/ 100 000,00 (cien mil y 00/100 soles), por la contratación de bienes y/o servicios iguales o similares al objeto de la adquisición.
		• Se consideran bienes y/o servicios similares los siguientes:
		  ○ Venta, suministro, renovación o suscripción de licencias de software antivirus.
		  ○ Venta o suscripción de soluciones de protección de endpoints.
		  ○ Implementación, configuración o soporte de soluciones EPP, NGAV, EDR, XDR o MDR.
		  ○ Venta o implementación de soluciones de seguridad para estaciones de trabajo, equipos portátiles o servidores.
		  ○ Venta o implementación de soluciones de protección contra malware o ransomware.
		  ○ Implementación de soluciones de control de dispositivos, control de aplicaciones, protección web, firewall de endpoint o gestión centralizada de endpoints.
		  ○ Servicios de soporte, mantenimiento o administración de soluciones de seguridad para endpoints.
		• La experiencia se acreditará mediante la presentación de uno o más de los siguientes documentos:
		  ○ Copia simple de contratos u órdenes de compra o servicio, conjuntamente con su respectiva conformidad, constancia de prestación o documento equivalente que acredite su ejecución.
		  ○ Comprobantes de pago cuya cancelación se acredite documentalmente mediante voucher de depósito, constancia de transferencia, reporte bancario, sello de cancelación u otro medio verificable.

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

		○ No se exigirá una cantidad mínima de contratos, órdenes o comprobantes de pago, siempre que la documentación presentada permita acreditar el monto facturado acumulado requerido.
	REQUIERE PERSONAL ESPECIALIZADO (EN CASO LA NATURALEZA DE LA ADQUISICON LO REQUIERA)	El proveedor deberá asignar como mínimo un (01) especialista responsable de la instalación, configuración, implementación, pruebas, transferencia de conocimientos y puesta en funcionamiento de la solución de seguridad para endpoints. **1. UN (01) ESPECIALISTA EN SEGURIDAD DE ENDPOINTS** **1.1. Formación académica:** • El especialista deberá contar con grado de bachiller o título profesional en alguna de las siguientes carreras: ○ Ingeniería de Sistemas. ○ Ingeniería Informática. ○ Ingeniería de Computación y Sistemas. ○ Ingeniería de Software. ○ Ingeniería de Redes y Comunicaciones. ○ Ingeniería de Telecomunicaciones. ○ Ingeniería Electrónica. ○ Ciencias de la Computación. ○ Informática. ○ Computación. ○ Otras carreras profesionales relacionadas con tecnologías de la información, redes, telecomunicaciones o ciberseguridad. • La formación académica deberá acreditarse mediante copia simple del diploma correspondiente. **1.2. Certificación técnica:** • El especialista deberá contar con una certificación técnica oficial vigente o constancia de capacitación emitida por el fabricante de la solución ofertada, relacionada con alguno de los siguientes ámbitos: ○ Administración de la solución. ○ Implementación y despliegue. ○ Protección de endpoints. ○ EPP, NGAV, EDR o XDR. ○ Seguridad de servidores y estaciones de trabajo. ○ Gestión y respuesta ante amenazas. • También se aceptarán certificaciones emitidas por centros de capacitación autorizados por el fabricante, siempre que se pueda verificar su correspondencia con la solución ofertada. **1.3. Formación complementaria:** • El especialista deberá contar con capacitación, curso, programa de especialización o diplomado en alguno de los siguientes ámbitos: ○ Ciberseguridad. ○ Seguridad de la información. ○ Seguridad informática. ○ Gestión de incidentes de seguridad. ○ Ethical hacking. ○ Administración de soluciones de seguridad. ○ Seguridad de redes. ○ Protección y respuesta ante amenazas. • La capacitación o especialización deberá tener una duración acumulada mínima de cuarenta (40) horas lectivas. **1.4. Experiencia del especialista:** • El especialista deberá acreditar una experiencia mínima acumulada de tres (03) años en actividades relacionadas con soluciones de seguridad para endpoints. • Se considerará válida la experiencia desempeñando uno o más de las siguientes funciones: ○ Especialista. ○ Ingeniero. ○ Analista.

Firmado digitalmente por
MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

		○ Consultor. ○ Administrador. ○ Implementador. ○ Coordinador. ○ Supervisor. ○ Jefe de proyecto. ○ Responsable técnico. ○ Soporte técnico especializado. • La experiencia deberá estar relacionada con una o más de las siguientes actividades: ○ Instalación, configuración o implementación de soluciones antivirus. ○ Implementación o administración de soluciones EPP, NGAV, EDR, XDR o MDR. ○ Protección de estaciones de trabajo, equipos portátiles o servidores. ○ Configuración de políticas de seguridad de endpoints. ○ Despliegue centralizado de agentes de seguridad. ○ Migración o reemplazo de soluciones antivirus. ○ Integración con Directorio Activo, SIEM, herramientas de monitoreo o plataformas de ciberseguridad. ○ Atención, investigación o respuesta ante incidentes de seguridad. ○ Asesoría, diagnóstico o soporte de plataformas de protección de endpoints. • La experiencia se acreditará mediante contratos y su respectiva conformidad, certificados, constancias de trabajo, constancias de prestación, órdenes de servicio con conformidad u otros documentos que permitan identificar las funciones realizadas y el periodo de participación del especialista.

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	La Entidad realizará un único pago a favor del proveedor, a la culminación de la instalación e implementación de la solución, previa revisión del informe técnico del mismo.	TOTAL DE PAGOS	01
	El OTASS cancelará dentro de los diez (10) días siguientes a otorgada la conformidad final por parte de la UTI, salvo que existan supuestos no contemplados que ameriten mayor tiempo al indicado, aspecto que el OTASS puede indicar al proveedor de considerarlo conveniente.			

8.	**PENALIDADES A APLICAR:**			
	TIPO DE PENALIDAD A APLICAR	Si el proveedor incurre en retraso injustificado en la entrega de los bienes o entregables definidos con plazos; la Entidad le aplicará automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula: $\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$ Donde: F = 0.25 para plazos mayores a sesenta (60) días o; F = 0.40 para plazos menores o iguales a sesenta (60) días. Tanto el monto como el plazo se refieren, según corresponda, al contrato vigente o ítem que debió ejecutarse.		
	FORMA DE CÁLCULO	$\textit{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$	MONTO MÁXIMO APLICABLE	10% del monto total de la contratación

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

	PENALIDADES ADICIONALES	No corresponde

9.	**CONDICIONES COMPLEMENTARIAS**	
	EMBALAJE, ROTULACIÓN O ETIQUETADO.	NO CORRESPONDE
	TRANSPORTE	NO CORRESPONDE
	ACONDICIONAMIENTO, MONTAJE E INSTALACIÓN	**1. IMPLEMENTACIÓN Y CONFIGURACIÓN DE LA SOLUCIÓN** 1.1. El proveedor deberá realizar una reunión de inicio, validar el inventario, arquitectura, conectividad, dependencias y coexistencia con herramientas actuales. 1.2. Deberá habilitar y asegurar la consola, crear roles, activar MFA, registrar licencias, configurar grupos, políticas base, exclusiones aprobadas, notificaciones, actualización y retención. 1.3. Deberá ejecutar un piloto representativo antes del despliegue masivo, incluyendo estaciones y equipos portátiles. 1.4. Deberá desplegar la solución en el porcentaje definido por la Entidad y entregar procedimientos o paquetes para despliegues posteriores. 1.5. Deberá validar, como mínimo, detección con archivo de prueba seguro EICAR o equivalente, generación de alertas, aislamiento, desaislamiento, control de USB, actualización, reportes y acceso por roles. 1.6. La configuración final deberá corresponder a recomendaciones del fabricante y al contexto del OTASS; no se aceptará dejar políticas predeterminadas sin revisión.
	CAPACITACIÓN Y/O ENTRENAMIENTO	• El proveedor brindará un mínimo de ocho (8) horas de capacitación para al menos dos (2) administradores designados por la Entidad. • La capacitación deberá cubrir arquitectura, operación de consola, políticas, despliegue, investigación EDR, aislamiento, respuesta, reportes, actualizaciones, solución de problemas y escalamiento. • Se entregará material digital y constancia o certificado emitido por el proveedor o fabricante, indicando participantes y horas realizadas.
	ACCESORIOS COMPLEMENTARIOS	NO CORRESPONDE
	MANTENIMIENTO PREVENTIVO	NO CORRESPONDE
	SOPORTE TÉCNICO	• El soporte técnico será 24x7 en español, con capacidad de escalamiento al fabricante durante toda la vigencia de las licencias. • El proveedor deberá proporcionar canales de atención por correo, teléfono y/o portal de tickets, así como procedimiento de escalamiento y matriz de contactos. • Para incidentes críticos que afecten masivamente la protección o disponibilidad, el tiempo máximo de primera respuesta del postor será de dos (02) horas dentro del horario de soporte. El escalamiento al fabricante deberá iniciarse sin demora cuando corresponda. • El proveedor deberá contar con al menos un especialista certificado o acreditado por el fabricante en la solución ofertada, o acreditar experiencia equivalente reconocida por el fabricante cuando este no disponga de certificación específica. • El soporte incluirá asistencia en políticas, actualizaciones, errores de agentes, incidentes de consola, exclusiones, reportes, integraciones incluidas y recuperación ante fallos de la solución. • Debe ser previsto un nivel de soporte directo con el fabricante que puede ser escalado de ser necesario por la Unidad de Tecnología de la Información del OTASS para casos críticos.
	MUESTRAS (De acuerdo a la naturaleza de los	NO CORRESPONDE

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

	bienes, se pueden requerir la presentación de muestra para la evaluación y verificación del cumplimiento de la especificación técnica).	
	GARANTIA COMERCIAL	**1. GARANTÍA DEL FABRICANTE:** 1.1. La solución ofertada deberá contar con garantía, suscripción, licenciamiento y soporte oficial del fabricante por un periodo mínimo de trescientos sesenta y cinco (365) días calendario, contado a partir del día siguiente de la suscripción del Acta de Implementación de la solución. 1.2. Durante dicho periodo, la Entidad deberá tener derecho, sin costo adicional, a: • Acceder a las actualizaciones de firmas, motores, modelos de detección, indicadores de compromiso, reglas de seguridad y demás componentes necesarios para la adecuada protección de los equipos. • Recibir correcciones de errores, parches, actualizaciones críticas y actualizaciones de seguridad. • Acceder a nuevas versiones, mejoras funcionales y versiones generales de mantenimiento liberadas por el fabricante para la edición o modalidad de licenciamiento contratada. • Acceder a la documentación técnica, manuales, notas de versión, base de conocimientos y demás recursos oficiales disponibles para la solución. • Mantener habilitadas todas las funcionalidades, módulos y capacidades consideradas en la oferta y requeridas en las especificaciones técnicas. • Acceder al soporte técnico oficial del fabricante, a través del proveedor o mediante los canales que este último habilite para la Entidad. • Escalar incidentes técnicos hacia los niveles especializados del fabricante cuando su complejidad lo requiera. 1.3. La garantía deberá cubrir todos los componentes, módulos, agentes, consolas, conectores y funcionalidades que formen parte de la solución ofertada. 1.4. El proveedor deberá acreditar la vigencia de la garantía, suscripción y soporte del fabricante mediante certificado, constancia, portal de licenciamiento, carta del fabricante, carta de un distribuidor autorizado u otro documento oficial equivalente. **2. GARANTÍA DEL PROVEEDOR:** 2.1. El proveedor deberá brindar garantía sobre los trabajos de instalación, configuración, implementación, integración, migración, despliegue, pruebas y puesta en operación de la solución durante toda la vigencia contractual. 2.2. La garantía del proveedor deberá cubrir, sin costo adicional para la Entidad: • La corrección de errores o deficiencias atribuibles a la instalación, configuración o implementación realizada. • La reconfiguración de políticas o parámetros que no funcionen de acuerdo con las especificaciones técnicas o con la oferta presentada. • La reinstalación o redespliegue de agentes cuando el inconveniente sea atribuible al procedimiento ejecutado por el proveedor. • La atención de incompatibilidades derivadas de una configuración incorrecta o incompleta. • El apoyo para el diagnóstico, apertura, seguimiento y escalamiento de casos ante el fabricante. • La aplicación de ajustes necesarios para mantener la operatividad de la solución.

		• La actualización de la documentación técnica cuando se realicen cambios sobre la configuración implementada. • La orientación y asistencia técnica a los administradores designados por la Entidad. 2.3. La garantía incluirá la atención de solicitudes de cambio relacionadas con las configuraciones implementadas por el proveedor, siempre que dichas solicitudes: • Se encuentren comprendidas dentro de las capacidades y funcionalidades licenciadas. • No impliquen la incorporación de nuevos productos, módulos, licencias o servicios no considerados inicialmente. • No constituyan una ampliación sustancial del alcance original de la solución. • No sean consecuencia de cambios realizados por terceros sin coordinación con el proveedor. 2.4. Las solicitudes de cambio podrán comprender, entre otras: • Creación, modificación o eliminación de políticas. • Configuración de grupos de equipos o usuarios. • Creación de exclusiones debidamente justificadas. • Ajustes en reglas de control de dispositivos, aplicaciones, navegación web o firewall. • Configuración de alertas, notificaciones, reportes y tareas programadas. • Ajustes en la integración con el Directorio Activo u otras herramientas consideradas en la implementación. • Modificaciones en los perfiles de acceso y roles administrativos. • Apoyo en el despliegue o reasignación de licencias por renovación o sustitución de equipos. 2.5. Toda modificación deberá ser previamente solicitada o autorizada por la Entidad y deberá quedar registrada en el correspondiente ticket, acta, informe o documento de atención.

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)	

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

	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, 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.

Firmado digitalmente por MINAYA CRUCES Daniel Manuel FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 11:57:51-0500

Firmado digitalmente por DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500

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 11:57:51-0500

Firmado digitalmente por
DONGO QUINTANA Alain Donuhue FAU 20565423372 soft
Motivo: Soy el autor del documento
Fecha: 2026/07/15 12:48:10-0500