Anexo N° 01

REQUERIMIENTO (Bienes y Servicios en general)	FOR-OGA-59 Versión 04

1	**DETALLE DE LA SOLICITUD**	
	DENOMINACION DE LA CONTRATACIÓN	Servicio de Renovación de Licencia de Software Antivirus
	FINALIDAD PÚBLICA	Salvaguardar la seguridad de la información de los equipos de cómputo e infraestructura de servidores con el fin de garantizar la integridad de los datos almacenados en la Entidad, asegurando la continuidad de las labores que permitan el cumplimiento de la misión de la ACFFAA.
	OBJETIVO DE LA CONTRATACIÓN	OBJETIVO GENERAL: Contar con licencias de antivirus actualizadas que permitan la protección del parque informático de la red de datos institucional, durante el plazo de ejecución contractual. OBJETIVO ESPECIFICO: - Contar con protección de virus informáticos en los servidores de la institución. - Contar con protección de virus informáticos en los computadores personales de la institución.
	ACTIVIDAD OPERATIVA (POI)	Gestión de las Tecnologías de Información
	FUENTE DE FINANCIAMIENTO	Recursos Ordinarios
	META PRESUPUESTARIA	Soporte y Aplicaciones de Tecnologías Informáticas

2	**ÁREA USUARIA**			
	UNIDAD DE ORGANIZACIÓN	OFICINA DE INFORMATICA		
	NOMBRE Y APELLIDOS	MAY DOMERGUE GUZMAN FUCHS		
	CORREO ELECTRÓNICO	mguzman@acffaa.gob.pe	CELULAR	933150888
	ÁREA TECNICA ESTRATÉGICA			
	UNIDAD DE ORGANIZACIÓN	OFICINA DE INFORMATICA		
	NOMBRE Y APELLIDOS	PASCAL VILLAVICENCIO FERNANDEZ		
	CORREO ELECTRÓNICO	pascal.villavicencio@acffaa.gob.pe	CELULAR	995960578

3 ALCANCES Y DESCRIPCIÓN GENERAL DEL SERVICIO

N°	DESCRIPCIÓN / NOMENCLATURA DEL BIEN O SERVICIO /	UNIDAD DE MEDIDA	CANTIDAD	CUBSO/FFTT (*)	SIGA
01	SERVICIO DE RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS	UNIDAD	1	8111250100334689	942500010040

(*) Agregar CUBSO; en caso de Fichas Técnicas aprobadas por Perú Compras, Fichas de Homologación o de naturaleza similar, consignar el código de la ficha vigente.

ACTIVIDADES/CARACTERISTICAS	Contratación de un servicio de renovación de 140 licencias de por el periodo de 1 año, con las siguientes características: **PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES**

		3.1. La consola de administración deberá ser de tipo nube, en modo Software as a Service permitiendo gestionarse desde la nube para equipos dentro y fuera de la red. 3.2. La consola de administración deberá poder lanzar tareas de despliegue de clientes de forma remota. 3.3. La consola de administración deberá poder mostrar un resumen de la instalación indicando el estado y sugiriendo una acción de refuerzo si fuese necesario. 3.4. La consola de administración deberá poder gobernar todos los antivirus residentes en las diferentes plataformas que tenga la institución Windows, Linux, Mac, Android, iOS y plataformas de virtualización como VMWare y Microsoft HyperV. 3.5. La consola deberá ser 100% web permitiendo implementar una nube privada o delegada a través un componente web seguro (https) a fin de poder gestionar estaciones de trabajo o Laptops que se encuentren fuera de la red corporativa de forma transparente. 3.6. La consola de administración deberá poder registrar eventos creando logs por cada uno de los eventos que realice dependiendo del ítem (exploración, actualización, bloqueos, etc.) 3.7. La consola de administración deberá permitir implementar exclusiones en la exploración, con capacidad para excluir de la exploración archivos, directorios y/o procesos, etc. De forma centralizada. 3.8. La consola de administración deberá permitir definir a través del residente acciones posteriores a la detección, capacidad para tomar distintas acciones cuando sea detectado un virus, o un ataque, limpiar el archivo infectado, moverlo a cuarenta, continuar la exploración, no tomar acción, eliminar el archivo, etc. 3.9. La consola de administración deberá permitir también definir acciones posteriores a la detección para una exploración bajo demanda, capacidad para tomar distintas acciones cuando sea detectado el virus, ataque o programa no deseado: limpiar el archivo infectado, moverlo a cuarentena, continuar la exploración, no tomar acción, eliminar el archivo, etc. 3.10. La consola de administración deberá permitir definir la exploración de correo electrónico con capacidad para exploración de mensajes de correo electrónico utilizando Microsoft Outlook, detención de virus y programas no deseados. 3.11. La consola de administración deberá permitir la programación de tareas, capacidad para programar tareas de exploración, actualización, etc. 3.12. La consola de administración deberá permitir la configuración de repositorios para actualización, capacidad para agregar/eliminar repositorios hacia donde se descarga la actualización de las definiciones de virus. 3.13. La consola de administración deberá permitir la instalación remota, pudiendo lanzar tareas de instalación en clientes de forma remota desde un servidor de administración antivirus. 3.14. La consola de administración deberá permitir crear usuarios con diferentes privilegios de acceso a la administración.

		3.15. La consola de administración deberá contar con una cuarentena local capaz de aislar posibles amenazas de malware no firmadas, pudiendo liberar y limpiar programas y/o aplicaciones según convenga el administrador. 3.16. La consola de administración deberá poder reportar y enviar directamente al fabricante software y/o amenazas no firmadas para su evaluación. 3.17. La consola de administración deberá poder integrarse con el directorio activo a fin de llevar una sola gestión (grupos organizativos) 3.18. La consola de administración deberá tener la capacidad de definir políticas de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para configuraciones de objetos específicos (Módulos de protección). 3.19. Este sistema deberá tener la capacidad de generar reportes locales en cada equipo referentes a todas las transacciones realizadas por cada producto. 3.20. La solución deberá incluir un sistema de análisis basado en algoritmos heurísticos capaces de detectar malware por similitud. 3.21. La solución deberá incluir un sistema que optimice la detección y eliminación de malware empaquetado usado para saturar el performance de los residentes antivirus lanzando miles de variables a partir de un malware ya conocido. 3.22. La solución deberá incluir tecnología basada en el análisis del comportamiento de amenazas logrando detenerlas incluso sin estar firmadas. 3.23. La solución deberá contar con un módulo dedicado al reconocimiento y detección de RANSOMWARE. 3.24. La solución deberá poder reconocer y bloquear amenazas de día cero basadas en vulnerabilidades del sistema operativo y programas instalados. 3.25. La solución deberá incluir tecnologías de Machine Learning que le permitan automatizar el aprendizaje de nuevas amenazas de malware a través de sus diferentes sensores o tecnologías propuestas. 3.26. La solución deberá tener un módulo que permita la implementación de políticas de seguridad para el control de aplicaciones, el mismo que deberá poder definir aplicaciones en lista negra para evitar que estas se ejecuten en las estaciones de trabajo y servidores de la red. 3.27. El módulo de control de aplicaciones deberá poder implementar sus políticas de aplicaciones en lista negras reconociendo el hash, versiones y fabricantes específicos de las aplicaciones a bloquear. 3.28. El módulo de control de aplicaciones deberá tener un modo que permita la implementación de políticas de seguridad para el control de aplicaciones el mismo que deberá poder definir aplicaciones en lista blanca que permitan que solo estas puedan ejecutarse en determinadas estaciones de trabajo y servidores. 3.29. El módulo de control de aplicaciones deberá poder aplicar políticas de seguridad a directorios y archivos específicos.

		3.30. El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su PC a fin de mejorar los tiempos de respuesta con el usuario. 3.31. La solución deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos extraíbles, el mismo que deberá poder ser desplegado, habilitado o deshabilitado desde la consola de administración. 3.32. El módulo de control de dispositivos deberá tener la capacidad de asignar privilegios de solo lectura a cualquier USB de almacenamiento externo que se conecte al equipo a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio. 3.33. El módulo de control de dispositivos deberá permitir que el usuario pueda solicitar permiso de acceso a su dispositivo desde su PC a fin de mejorar los tiempos de respuesta con el usuario. 3.34. El módulo de control de dispositivos deberá permitir la creación de listas blancas especificas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento. 3.35. La solución deberá tener un módulo que permita la implementación de políticas de seguridad para la navegación web el mismo que no debe necesitar instalar ningún tipo de plugin o componente adicional para escanear y filtrar contenido en los navegadores (Browsers soportados, Internet Explorer, Firefox y Chrome). 3.36. El módulo de filtro web debe proveer al administrador la facultad de definir filtros en base a categorías para la navegación de los usuarios finales conectados o desconectados de la red. Estas categorías deben comprender sexo, pornografía, navegadores anónimos, desnudos, redes sociales, música, videos y otros. Además, debe permitir ingresar páginas web específicas para permitir como excepción o bloquear adicionalmente. 3.37. El módulo de acceso a internet deberá permitir definir días, horas de acceso a internet para determinados grupos o PCs en particular. 3.38. La solución deberá mitigar el daño provocado por contagios; cierra los puertos, monitorea aplicaciones y motores de correo electrónico, analice archivos y carpetas, que efectúe seguimientos y bloquee las comunicaciones que generen una infección. 3.39. La solución deberá incluir protección que amenace específicamente las vulnerabilidades del sistema operativo, deberá incluir protección anti-exploit capaz de proteger de esas amenazas que aprovechan las brechas de seguridad en los programas instalados, desde editores de texto hasta plugins de los navegadores. 3.40. El módulo de gestión de parches deberá ser capaz de realizar tareas de rollback (desinstalación remota de parches desde consola) en caso de requerirse. 3.41. Si el administrador así lo prefiere se podrá habilitar opción de desactivar cortafuego desde el cliente. 3.42. La solución debe incluir tecnología innovadora para PC y Servidores que detenga y elimine proactivamente el software malicioso, extienda la

		cobertura contra nuevos riesgos de seguridad y reduzca el costo de respuesta frente a epidemias. 3.43. La solución debe permitir defender los sistemas contra virus, gusanos, troyanos, phishing, adware y spyware. 3.44. La solución debe bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria. 3.45. La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexión con servidores maliciosos de comando y detectar patrones típicos de equipos que forman parte de una Botnet. 3.46. La solución deberá contar con protección contra ransomware que supervise el comportamiento de las aplicaciones y los procesos que intentan modificar los datos. 3.47. La solución deberá bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica. 3.48. La solución deberá proteger contra exploits dirigidos a aplicaciones y servicios Microsoft, especialmente a servicios del sistema operativo Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft Outlook. 3.49. La solución debe incluir un antivirus residente capaz de analizar diferentes protocolos de comunicación como HTTP, HTTPS, SMPT, POP, IMAP y otros. 3.50. El residente antivirus deberá poder tomar diversas acciones en caso de una infección, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo. 3.51. El residente antivirus deberá poder tomar diversas acciones en caso de analizar archivos comprimidos, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo. 3.52. El residente de antivirus deberá poder configurarse en acceso a lectura, escritura y al ejecutar para que se esta manera se tenga mejor visibilidad de todos los archivos que se escriban en disco. 3.53. El residente de antivirus deberá poder comprobar la existencia de virus informáticos en correos recibidos / enviados en el cliente de correo. Adicionalmente se podrá realizar la comprobación solo en los correos no leídos. 3.54. El residente de antivirus deberá poder adjuntar un informe de ante un correo electrónico infectado. 3.55. El residente deberá detectar y neutralizar amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes. 3.56. El residente deberá contar con una tecnología capaz de informar a través de internet acerca de ciertas concentraciones de correos sospechosos cerrando prácticamente en tiempo real la brecha que existe entre el comienzo de un envío masivo de correos y su bloqueo mediante las firmas de virus adaptadas especialmente para ese virus.

		3.57. La solución debe permitir crear un CD, DVD o USB de arranque para efectuar un análisis completo de un equipo o servidor, este análisis se debe realizar antes de que arranque el sistema operativo instalado y utilizar firmas de virus actualizadas, esto a fin de recuperar un sistema infectado. 3.58. La solución debe ser capaz de que cada vez que identifique un problema, debe permitir corregir los problemas de forma remota, con al menos las siguientes opciones: a. Proteger el dispositivo con la opción de inicio de una exploración. b. Forzar una actualización en ese momento. c. Ver los detalles de los eventos ocurridos. d. Ejecutar la comprobación completa del sistema. e. Forzar el cumplimiento de una nueva política de seguridad. f. Mover el equipo a otro grupo. g. Borrar el equipo de la lista. h. Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro manualmente o automáticamente. 3.59. La consola deberá poder grabar un registro de auditoria seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorias de seguridad, análisis y solución de problemas forenses. 3.60. Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF. 3.61. Debe contener varios informes para el análisis y control de los usuarios y endpoint. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoint. 3.62. Debe permitir la ejecución manual de todos estos informes, así como la programación y envió automático por correo electrónico en los formatos CSV y PDF. 3.63. Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda. 3.64. Deberá tener la posibilidad de instalar un servidor para reenvío de eventos en caso de que el agente no pueda comunicarse con la consola en la nube. 3.65. La protección debe poder detectar malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido. 3.66. Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque. 3.67. Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables. 3.68. Debe proteger las funciones críticas en los navegadores de Internet. 3.69. Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.

		3.70.	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas.
		3.71.	Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
		3.72.	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
		3.73.	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
		3.74.	Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
		3.75.	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
		3.76.	Detección proactiva de reconocimiento de nuevas amenazas:
		3.77.	Protección de amenazas de día O a través de tecnología de Deep learning.
		3.78.	Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep learning.
		3.79.	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
		3.80.	Capacidad de detección y Noqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
		3.81.	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
		3.82.	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
		3.83.	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas.
		3.84.	Generación de excepciones ante falsos positivos.
		3.85.	Disponer de capacidad de protección contra ransomwares no basada exclusivamente en la detección por firmas.
		3.86.	Disponer de capacidad de remediación de la acción de encriptación maliciosa de los ransomwares.
		3.87.	Para servidores, disponer de capacidad de prevención contra la acción de encriptación maliciosa ejecutada por ransomwares, posibilitando aún el bloqueo de las computadoras de donde parte tal acción.
		3.88.	Debe poseer protección anti-ransormwares para el sector de booteo de restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomwares.
		3.89.	Debe informar a la consola todo el detalle del incidente para analizar la causa raíz de manera efectiva.
		3.90.	Protección contra vulnerabilidades y técnicas de explotación:

		a. Detección y protección de técnicas de explotación de DLL Injection. b. Mitigación de inyección de códigos en procesos. c. Protección contra robo de credenciales. d. Protección contra malware oculto en aplicaciones legitimas (code cave). e. Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro. f. Evitar obtener escalada de privilegios y acceso elevado a recursos. g. Modificación de claves de registro para la ejecución de código arbitrario. Otros Alcances: - El servicio de renovación deberá contemplar la cobertura de antivirus desde el 05-09-2026 hasta el 04-09-2027. - El proveedor deberá confirmar la integración del software antivirus con el AD, así como la generación de agentes para su posterior instalación en los equipos (Windows o Linux). - El servicio de renovación debe incluir lo siguiente: • Soporte mediante línea telefónica, correo electrónico o en sitio cuando se requiera en modalidad de 24 x 7 x 365. • Soporte de segundo nivel dado por el Fabricante, con un tiempo de respuesta, no mayor de cuatro (04) horas y un tiempo de solución no mayor de tres (03) horas. • Soporte de segundo nivel dado por el fabricante a través de correo electrónico, teléfono y chat 24x7. • Durante la vigencia del licenciamiento, la ACFFAA siempre deberá contar con las últimas versiones o actualizaciones de la solución. • El contratista, deberá brindar entrenamiento virtual o presencial para el personal técnico de la Oficina de Informática, la cual debe ser de un total de cinco (05) horas y para tres (03) personas como mínimo de la Oficina de Informática, las constancias de capacitación deberán ser presentadas dentro del informe técnico. • El horario y lugar deben ser coordinados con la Oficina de Informática, a través del correo electrónico pascal.villavicencio@acffaa.gob.pe entrenamiento debe considerar los siguientes temas: - Instalación - Configuración - Administración de la solución ofertada - Solución de problemas sobre los componentes de la herramienta • El contratista deberá incluir archivos digitales (separatas, manuales y/o videos) enviado a pascal.villavicencio@acffaa.gob.pe, los cuales deberán ser referidos a la configuración, instalación y administración del servicio, dicha evidencia del envió deberá ser incluido en el Informe técnico.
	PLAN DE TRABAJO (DE CORRESPONDER)	No Corresponde

	RECURSOS A SER PREVISTOS POR EL PROVEEDOR	No Corresponde
	RECURSOS A SER PREVISTOS POR LA ENTIDAD	No Corresponde
	PRESTACIONES ACCESORIAS A LA PRINCIPAL	
	MANTENIMIENTO PREVENTIVO Y/O CORRECTIVO	No Corresponde
	SOPORTE TECNICO	Sera de un (01) año, contabilizados a partir del Acta de Conformidad emitida por la ACFFAA.
	CAPACITACIÓN Y/O ENTRENAMIENTO	cinco (05) horas y para tres (03) personas como mínimo de la Oficina de Informática.
	OTRAS CARACTERISTICAS/CONDICIONES	No Corresponde

4	**LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO**	
	LUGAR DE LA PRESTACIÓN	El servicio se realizará en forma virtual y/o presencial para la Agencia de Compras de las Fuerzas Armadas sito Av. Arequipa 310 – Cercado de Lima.
	PLAZO DE PRESTACION	365 días a partir del 05-09-2026

5	**ENTREGABLES (OBLIGATORIO)**	
	NUMERO DE ENTREGABLES	Único
	CONTENIDO DE CADA ENTREGABLE	<u>El contratista deberá presentar una carta adjuntando:</u> - Documento de registro del software antivirus del fabricante a nombre de la Agencia de Compras de las Fuerzas Armadas (ACFFAA), donde se especifiquen ciento cuarenta (140) licencias de la solución ofertada y acredite la vigencia. - Documento emitido por el contratista en la que detalla la garantía. - Constancia de entrenamiento (versión física o digital) otorgados por el Contratista de un total de cinco (05) horas y para dos (02) personas designadas por la Oficina de Informática. - Informe técnico de la implementación realizada. - El comprobante de pago de la solución ofertada. - Carta indicando números de contacto para soporte técnico.
	PLAZO DE PRESENTACIÓN	A los 3 días máximo de culminado el servicio
	LUGAR DE PRESENTACIÓN DE LOS ENTREGABLES	El servicio se realizará en forma virtual y/o presencial para la Agencia de Compras de las Fuerzas Armadas sito Av. Arequipa 310 – Cercado de Lima.
	OTRAS CONDICIONES	No Aplica

6	**PENALIDADES POR APLICAR**	
	PENALIDAD POR MORA	"En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 140 del Reglamento de la Ley 32069".
	FORMA DE CÁLCULO	Penalidad diaria = 0.10 x monto del contrato, ítem o entregable correspondiente / F x plazo del contrato, ítem o entregable correspondiente Donde F tiene los siguientes valores: Para bienes y servicios: F = 0.40
	OTRAS PENALIDADES	No Aplica

OTRAS PENALIDADES			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento de verificación

7	**REQUISITOS MÍNIMOS DEL PROVEEDOR Y/O PERSONAL PROPUESTO**	
	EXPERIENCIA DEL PROVEEDOR	- Personal Natural o Jurídica - Contar con RUC, activo y habido - Contar con Registro Nacional de Proveedores (RNP) vigente. Mínimo de tres (03) servicios relacionadas al objeto de la contratación; La experiencia del postor se acreditará con copia simple de: (i) contratos y órdenes de compra-servicios con su respectiva conformidad o constancia de prestación; (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con vouchers de depósito, nota de abono, reporte de estado de cuenta, y/o cualquier otro documento emitido por Entidad del Sistema Financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago correspondientes. Se consideran servicios similares a los siguientes: Servicio de renovación de software y/o venta de software de seguridad.
	EXPERIENCIA DEL PERSONAL CLAVE	• El personal técnico que realizará el servicio deberá contar con capacitación en implementación de software antivirus o similares, se acreditará con copia simple.
	FORMACIÓN ACADÉMICA	No Aplica
	CAPACITACIÓN	cinco (05) horas y para dos (02) personas como mínimo de la Oficina de Informática, las constancias de capacitación deberán ser presentadas dentro del informe técnico
	OTROS	No Aplica

8	**CONFORMIDAD DE LA PRESTACION**

	UNIDAD USUARIA QUE BRINDARA LA CONFORMIDAD	La Oficina de Informática
	PROCEDIMIENTO Y REQUISITOS A CUMPLIR POR EL PROVEEDOR	El servicio debe quedar 100% operativo, sin observaciones
	La conformidad se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. La conformidad es otorgada en el plazo máximo de SIETE (7) DÍAS CALENDARIO, contados desde el día siguiente de recibido el entregable.	

9	**PAGO DE LA PRESTACION**	
	FORMA DE PAGO	Único pago
	DOCUMENTOS	✓ Factura ✓ Documentos detallados en el entregable, ítem 5 ✓ Carta de garantía
	El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del contratista en un plazo máximo de diez (10) días hábiles luego de otorgada la conformidad por parte del Área Usuaria, salvo que existan supuestos no contemplados que ameriten mayor tiempo al indicado, aspecto que la ACFFAA podrá indicar al Contratista de considerarlo conveniente.	

10	**CLAUSULA DE CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL (DE CORRESPONDER)**
	EL CONTRATISTA se sujeta a la confidencialidad y reserva absoluta de la información y documentación relacionada con la prestación a la que tenga acceso, quedando expresamente prohibido revelar dicha información a terceros. EL CONTRATISTA debe dar cumplimiento a todas las políticas y estándares definidos por LA ACFFAA, en materia de seguridad de la información. Esta obligación comprende la información que se entrega, como también la que se genera durante la realización del servicio y la información producida una vez que se haya concluido la prestación. Dicha información y material puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos producidos en medios escritos, magnéticos, digitales y demás datos compilados o recibidos por EL CONTRATISTA. La documentación generada por el servicio pasará a ser propiedad de la ACFFAA.

11	**REPONSABILIDAD POR VICIOS OCULTOS**
	El plazo máximo de responsabilidad del contratista es de **UN (1) AÑO** contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.
	La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y 144 de su Reglamento aprobado por Decreto Supremo N° 009-2025-EF.

12	**CLAUSULA DE CUMPLIMIENTO**
	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 a la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, 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.

	CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO
13	A la suscripción de este contrato, EL CONTRATISTA 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 CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, 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 CONTRATISTA 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 CONTRATISTA 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 con LA ENTIDAD CONTRATANTE. Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

	SOLUCION DE CONTROVERSIAS
14	Las controversias que surjan entre las partes durante la ejecución e interpretación de la presente contratación se resuelven mediante, conciliación, según el acuerdo de las partes. Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas

15	**OTRAS CONDICIONES**

	SUSCRIPCIÓN DEL REQUERIMIENTO	
16	ACFFAA AGENCIA DE COMPRAS DE LAS F.F. A.A. Firma Digital Firmado digitalmente por VILLAVICENCIO FERNANDEZ Pascal FAU 20556939781 hard Motivo: Soy el autor del documento Fecha: 27.02.2026 11:46:03 -05:00	ACFFAA AGENCIA DE COMPRAS DE LAS F.F. A.A. Firma Digital Firmado digitalmente por GUZMAN FUCHS May Domergue FAU 20556939781 hard Motivo: Soy el autor del documento Fecha: 27.02.2026 14:23:52 -05:00
	FIRMA DEL ESPECIALISTA ÁREA USUARIA	**FIRMA DEL ENCARGADO ÁREA USUARIA**
	LUGAR Y FECHA	LIMA, 27 de febrero del 2026

	FIRMA RESPONSABLE DEC

17	**OBSERVACIONES:** DE CORRESPONDER	
	LUGAR Y FECHA	