

**TÉRMINOS DE REFERENCIA
PARA LA SUSCRIPCIÓN DE LICENCIAS ANTIVIRUS Y SOPORTE TÉCNICO**

1. DEPENDENCIA SOLICITANTE

Oficina de Tecnologías de Información.

2. FINALIDAD PUBLICA

El parque informático de la Superintendencia Nacional de Servicios de Saneamiento (En adelante SUNASS), sirve como herramienta tecnológica de soporte, a los trabajadores de la entidad, para el cumplimiento de las labores encomendadas en beneficio del público en general. Para este fin, se requiere que este parque informático cuente con protección de software para prevenir ataques mediante virus informáticos a nivel de estaciones de trabajo y servidores.

3. OBJETIVO DEL SERVICIO

Suscripción de licencias antivirus y soporte técnico, para ser utilizado en los equipos de cómputo (servidores, desktops y laptops) del personal y servidores físicos y/o virtuales de SUNASS.

4. VINCULACIÓN POI

Adquisición y renovación de software

5. FUENTE DE FINANCIAMIENTO

RO (Recursos Ordinarios)

6. BASE LEGAL APLICABLE

Marco normativo vigente emitido por la Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros – PCM, con el fin de garantizar la continuidad de los servicios de información.

- RESOLUCIÓN DIRECTORAL N° 056-2017-INACAL/DN, de fecha 29 de diciembre de 2017, aprueban la Norma Técnica Peruana, NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1a Edición.

7. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

ITEM UNICO	DESCRIPCIÓN	CANT
	SUSCRIPCIÓN DE LICENCIAS ANTIVIRUS Y SOPORTE TECNICO	1000

La suscripción de Licencias Antivirus comprende lo siguiente:

- La solución deberá presentarse en modalidad de suscripción y deberá brindarse desde la nube del fabricante o proveedor autorizado.
- La solución deberá permitir que las actualizaciones y definiciones de virus se programen de manera automática y periódicamente.
- [De manera opcional](#), la solución deberá poder integrarse con un módulo de gestión y distribución de parches de sistema operativo y aplicaciones instaladas que permita cerrar brechas de seguridad basadas en este tipo de vulnerabilidades.
- Las licencias de antivirus deberán ser administrada desde una consola central, del mismo producto la cual se debe tener acceso a través de un navegador web estándar y/o sistema integrado de gestión móvil que permita establecer conexión segura con la consola en la nube.
- En los reportes generados por ésta se deberá visualizar el ranking de los virus encontrados, de los

equipos desinfectados e infectados, la fecha y versión de la actualización, de las versiones de los motores, archivo infectado y nombre del virus y otras características necesarias para poder realizar el análisis de la red interna.

- La consola deberá tener la factibilidad de instalarse sobre los sistemas operativos de estaciones de trabajo: MS Windows 10, Windows 7 o superiores, así como en Windows Server.
- La consola deberá buscar estaciones de trabajo y servidores desprotegidos de la red y deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registro) además de generar reportes, estadísticas, gráficos configurables que puedan ser exportados a diferentes formatos.
- La consola deberá proveer informes automáticos y personalizables para supervisar las actividades del motor antivirus.
- El despliegue de la solución ha de requerir el uso de un único agente el cual debe ser administrado y gestionado por la consola central de administración. Se debe tener la posibilidad de desinstalar el antivirus en forma desatendida y remota.
- La configuración debe contar con una protección que no permita ser modificada o desactivada por el usuario.
- Debe tenerse la posibilidad de buscar (detectar y eliminar) virus (y sus variantes) en protocolos POP3, HTTP, SMTP, IMAP, NNTP.
- Permitir una actualización instantánea sin necesidad de la implementación de software adicional en cada punto final (estaciones de trabajo y servidores).
- Ser capaz de detener programas maliciosos y sus variantes, así como gusanos, troyanos, software espía, software de publicidad no deseado, adware, spyware, PornDial/Diales, keyloggers, bots, macrovirus, amenazas de día cero y rootkits en todos los archivos o tipos de archivo, residentes en memoria, comprimidos (cualquier formato de compresión) a diferentes niveles, ocultos y archivos en ejecución.
- Debe integrar un sistema capaz de monitorear el comportamiento y almacenar cada acción, acciones que incluyen acceso al sistema de archivos, al registro, conexiones de red y comunicación entre procesos a fin de que cada vez que se agregue algo a la base de datos de gráficos, se pueda buscar en el gráfico un comportamiento malicioso basado en patrones.
- Este sistema de monitoreo de comportamiento debe ser 100% automático pudiéndose habilitar o deshabilitar desde consola.
- Proporcionar informes unificados y centrales. El licenciamiento y mantenimiento también han de ser unificados.
- Reducir la carga administrativa a través de una interfaz de administración sencilla, confiable y de fácil uso.
- Realizar un análisis proactivo de amenazas en base a comportamientos buenos y malos de las aplicaciones desconocidas proporcionando una detección más precisa del software malicioso y sus variantes.
- La detección de software malicioso y sus variantes deberá poder hacerse sin la necesidad de realizar configuraciones basadas en normas.
- La solución antimalware deberá incluir una protección contra dispositivos USB físicos manipulados o infectados.
- Tener la capacidad de reducir los falsos positivos.
- Tener la capacidad de detección y eliminación avanzada de rootkits mediante el acceso por debajo del sistema operativo (background).
- Permitir al administrador controlar el acceso a procesos, archivos y carpetas específicas creadas por los usuarios y otras aplicaciones. Asimismo, debe permitir el análisis de aplicaciones, control de accesos, control de acceso al registro, archivos, control de módulos y librerías DLL.

- Permitir a los administradores restringir actividades consideradas sospechosas o de alto riesgo.
- Tener la funcionalidad de evitar la propagación de software malicioso y sus variantes antes de que comprometan la operatividad de los puntos finales (estaciones de trabajo y servidores).
- Tener la funcionalidad de bloquear los puntos finales (estaciones de trabajo y servidores) para prevenir la fuga de datos.
- Evitar que la información considerada confidencial sea extraída o robada de los puntos finales y evitar que software malicioso infecte los puntos finales desde los dispositivos periféricos.
- Los análisis, revisiones, scans que la solución haga no deben afectar el rendimiento ni la performance de los puntos finales (estaciones de trabajo y servidores). Asimismo, el consumo de memoria debe ser el mínimo posible.
- La protección contra código espía y sus variantes debe ser en tiempo real minimizando todos los riesgos posibles de posible infección del punto final (estaciones de trabajo y servidores) no comprometiéndolo el rendimiento de éste.
- Permitir la definición y configuración de exclusiones para servicios y aplicaciones corporativas. Asimismo, se debe permitir el uso de exclusiones comunes.
- Las firmas de la solución deben actualizarse permanentemente y debe tener la opción de hacerlo localmente, mediante la red y web del fabricante.
- La protección que la solución brinde deberá ser proactiva en todos sus módulos.
- La solución deberá permitir el manejo, gestión y administración de dispositivos de tipo USB, Dispositivos de Almacenamiento Externo. Asimismo, debe permitir el bloqueo de dispositivos periféricos por "class ID".
- La solución deberá tener la capacidad de auditar y de bloquear la lectura, escritura y ejecución de dispositivos removibles, CD/DVD drives, discos duros y unidades de red potencialmente peligrosas o riesgosas.
- El control de los dispositivos de almacenamiento masivo (USB's, CD/DVD) no debe requerir instalar otra herramienta, sino que debería ser parte de la solución.
- La solución deberá presentar una interfaz de usuario simplificada, entendible, de fácil integración a entornos de trabajo propietarios y de sencillo despliegue en distintos tipos de organizaciones.
- [De manera opcional](#), la solución debe tener la capacidad de análisis de tráfico VPN encriptado y des encriptado a través del mapeo específico de puertos.
- La solución antimalware deberá incluir tecnologías de detección antivirus basada en inteligencia artificial y machine learning.
- La solución antimalware deberá incluir tecnología de análisis de malware como motor de detección basado en firmas para la detección y eliminación de malware reconocido, así como análisis heurístico, para el reconocimiento y eliminación de malware no reconocido y supervisión de conducta para el reconocimiento de amenazas de día cero.
- La solución antimalware deberá incluir uno o dos motores de análisis de virus de diferentes fabricantes en el mismo software, lo que se busca es que la solución incremente el nivel de detección de malware.
- La solución antimalware deberá poder detectar y eliminar amenazas de tipo Ransomware.
- La solución deberá poder revertir una tarea de cifrado de archivos no autorizado.
- La solución deberá mostrar diagrama de causa raíz para los problemas que identifique.
- La solución deberá incluir un módulo de control de aplicaciones capaz de poder definir aplicaciones en LISTA NEGRA (lista que permite bloquear aplicaciones) para evitar que estas se ejecuten en las estaciones de trabajo y servidores de la red.
- La solución deberá incluir un módulo de control de aplicaciones capaz de poder definir aplicaciones en LISTA BLANCA (lista que permite ejecutar aplicaciones) que permitan que solo estas puedan ejecutarse en determinadas estaciones de trabajo y servidores.
- La solución deberá incluir un módulo de control de aplicaciones capaz de reconocer el hash o MD5 de

la aplicación a bloquear, así como extender el criterio de bloqueo a versiones y fabricantes específicos.

- El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su PC.
- La solución deberá contar con una tecnología que le permita lanzar escaneos de malware en modo de reposo, de esta forma se aprovecharían los tiempos muertos del usuario para escanear la PC en busca de malware sin castigar los recursos cuando el usuario los necesita o alguna estrategia similar que cumpla con el mismo objetivo.
- La solución debe integrar un módulo protección contra ataques que buscan obtener acceso al sistema explotando las vulnerabilidades específicamente de la red, ampliando las áreas protegidas, ahora con una seguridad basada en la red que bloquea, antes de que puedan ejecutarse, amenazas como los ataques de fuerza bruta, el robo de contraseñas, los exploits de red y movimientos laterales.
- La solución debe integrar un sistema de análisis y gestión de riesgos cibernéticos que permita identificar, evaluar y reparar eficazmente las debilidades de los endpoints para desarrollar un buen programa de seguridad y reducir los riesgos en la organización.
- La solución de gestión de riesgos integrada a los endpoints deberá reducir la exposición y endurecer la superficie del endpoint mediante la detección y priorización de peligrosas configuraciones erróneas del sistema operativo y del software.
- La solución debe integrar una plataforma de gestión de riesgos capaz de mostrar un panel donde se presente el score o puntaje que determina el riesgo al que se exponen los activos de TI protegidos.
- La solución debe integrar una plataforma de gestión de riesgos capaz de considerar mínimamente parámetros como seguridad de los navegadores, seguridad de la red basado en credenciales, vulnerabilidades del sistema operativo y vulnerabilidades que derivan de las aplicaciones instaladas.
- La solución de integrar una plataforma de gestión de riesgos capaz de analizar las acciones de los usuarios a través de un sistema de análisis de riesgos basado en comportamiento del usuario, identificando comportamientos que pueden llegar a suponer un riesgo de seguridad tanto para la organización como para el propio usuario. Esta funcionalidad debe actualizarse a través de un motor de análisis de riesgos de la misma plataforma, permitiendo obtener una visión integral del posicionamiento real de seguridad de la entidad.
- La solución debe integrar una plataforma capaz de presentar graficas de resumen con información relacionada a la severidad de las vulnerabilidades, TOP de aplicaciones más vulneradas, TOP de riesgo humano más crítico y TOP de usuarios más vulnerables.
- La solución debe integrar una base de conocimientos sobre tácticas y técnicas que utilizan los adversarios o ciberdelincuentes perpetrar sus ataques, estas deberán estar alineadas a MITRE ATT&CK.
- La solución deberá establecer porcentaje de riesgo puntual en función a vulnerabilidades, configuraciones de usuarios, actividad de la red y configuración de aplicaciones.
- La solución deberá proteger entornos virtualizados.
- La solución deberá poder reconocer todos los programas instalados en los equipos y priorizarlos por sus vulnerabilidades.
- La solución deberá poder integrar cuando se necesite de forma nativa funcionalidades adicionales de gestión avanzada de parches.
- La solución podrá definir relay de actualización desde el panel de control en la nube.
- La solución deberá incluir una plataforma integrada para gestión, prevención y mitigación de amenazas cibernéticas los servidores críticos de la entidad.
- La solución debe integrar tecnología para detectar y responder a las amenazas basadas en el host mediante el análisis del tráfico de red.
- La solución de análisis de trafico de red debe utilizar machine learning y heurística para analizar el comportamiento en tiempo real con el fin de descubrir con precisión actividades de MALWARE como

movimientos laterales e intentos de fuerza bruta.

- La solución deberá incluir defensa contra ataques de red para reforzar protocolos como HTTP, SMB, RPC y analizar el tráfico de red para bloquear ataques como los de inyección de código SQL, fuerza bruta y descargas ocultas.
- La solución deberá impedir acceso a las credenciales de los Endpoints implementando una defensa contra ataques de red evitando la filtración a fin de proteger la información confidencial frente a los delincuentes informáticos que utilizan técnicas como el registro de pulsaciones de teclas o el volcado de credenciales para robar nombres y contraseñas de cuentas.
- La solución deberá contar con soporte local de primer nivel a cargo del contratista, la disponibilidad del servicio deberá ser 24x7x365.
- Si se identifica que, de la instalación del software de antivirus, los equipos de cómputo y/o servidores y/o equipos de comunicación se ven afectados, el proveedor deberá garantizar la continuidad de las operaciones y mantener el orden establecido en la infraestructura de red y comunicaciones.
- Todo el esquema de licenciamiento ofertado debe estar a nombre de SUNASS para lo cual se deberá considerar el uso de la cuenta licencias@sunass.gob.pe

Servicio de Soporte técnico

- i. El contratista deberá proporcionar un número telefónico y correo electrónico para contactar a su mesa de ayuda y los niveles de escalamientos de incidentes. La mesa de ayuda debe estar disponible de lunes a domingo (24 x 7x 365), durante el tiempo de prestación del servicio.
- ii. La SUNASS reportará un incidente de ser el caso, vía telefónica y/o correo electrónico, considerándose todas estas formas igualmente válidas. Finalizado el reporte de la incidencia, el contratista deberá proporcionar un código de incidencia para el seguimiento de esta. Posteriormente, a solicitud de la SUNASS, el contratista deberá proporcionar información del estado del incidente reportado, a través de correo electrónico que será proporcionado por la oficina de tecnologías de la información (OTI).
- iii. Se instalará los parches y/o actualizaciones conforme se vayan publicando por el fabricante.

8. REQUISITOS DEL CONTRATISTA

- Persona natural o jurídica que brinde el servicio de suscripción de licencias antivirus y soporte técnico. Debe estar acreditado por el fabricante o representante local oficial de la marca ofertada.
- Contar con Certificación SOC2 de tipo 2. La certificación Service Organization Control 2 (SOC2) de tipo 2 deberá validar la superación de auditorías anuales según las directrices de AICPA SSAE- 16 SOC 2 respecto a seguridad, confidencialidad y disponibilidad, de la solución propuesta.

9. REQUERIMIENTO DE PERSONAL DEL CONTRATISTA

PERSONAL CLAVE

JEFE DE PROYECTO (01)

Funciones:

- Diseñar, Planificar y Auditar las actividades para la implementación de la plataforma requerida, las cuales serán:
 - ✓ Analizar la situación actual de la SUNASS
 - ✓ Definir el equipamiento para detección y respuesta de ciberataques.

- ✓ Coordinar las actualizaciones de los sistemas y aplicaciones.
- ✓ Implementar políticas de ciberseguridad.

Debe contar con las siguientes certificaciones:

- ✓ Certificación en IT Service Management – ITIL Foundation Certificate.
- ✓ Certificación vigente en Project Management Professional (PMP).
- ✓ Certificación oficial emitida por el fabricante como “Técnico Especialista del Portafolio De La Solución Ofertada”. (opcional)

PERSONAL DE SOPORTE (01)

Funciones:

- Apoyar, asistir y soportar técnicamente en la implementación y el mantenimiento del servicio.
- Brindar asistencia técnica de manera remota.
- Apoyar en el despliegue de la solución.

Debe contar con la siguiente certificación:

- ✓ Certificación oficial emitida por el fabricante como “Técnico Especialista del Portafolio De La Solución Ofertada”.

PERSONAL DE IMPLEMENTACIÓN (01)

Funciones:

- Apoyar y asistir técnicamente en la implementación del servicio.
 - ✓ implementación del servidor en el caso sea Onsite, (los recursos, de Ram, Procesador, espacio de disco, Sistema Operativo).
 - ✓ Implementación del despliegue de los agentes en los equipos de cómputo de los usuarios
 - ✓ Identifica medidas de seguridad adecuadas para la organización

Debe contar con la siguiente certificación:

- ✓ Certificación oficial emitida por el fabricante como “Técnico Especialista del Portafolio De La Solución Ofertada”.

10. LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio será brindado en la sede central de la SUNASS, ubicada en la Av. Bernardo Monteagudo N° 210, ciudad de Lima – Magdalena del Mar.

11. PLAZO DE ACTIVACIÓN Y VIGENCIA DEL SERVICIO

TABLA N° 01

Grupos de activación	Plazo de entrega	Vigencia del servicio
1er Grupo (500 suscripción de licencias y soporte técnico).	Hasta 10 días calendario, contabilizados a partir del día siguiente de suscrito el contrato. El servicio deberá activarse el día 23.12.24	12 meses contabilizados a partir de la fecha señalada en el documento de activación.

2do grupo (500 suscripción de licencias y soporte técnico).	El servicio deberá activarse el día 03.05.25	12 meses contabilizados a partir de la fecha señalada en el documento de activación.
---	--	--

12. ENTREGABLES

El contratista deberá entregar la documentación que acredite la activación de la suscripción de Licencias Antivirus y soporte técnico, de acuerdo con lo señalado en el numeral 11 de los Términos de Referencia.

Al inicio del primer grupo de activación

- Documento de activación de 500 de licencias y soporte técnico.
- Informe técnico sobre el estado actual de la plataforma de Antivirus y sobre el número de equipos desplegados y actualizados, así como el estado de los equipos que se encuentran enrolados a la consola de antivirus.
- Documento que indique la fecha de activación de 500 licencias y soporte técnico.

Al inicio del segundo grupo de activación

- Activación de 500 licencias y soporte técnico.
- Informe técnico sobre el estado actual de la plataforma de Antivirus y sobre el número de equipos desplegados y actualizados, así como el estado de los equipos que se encuentran enrolados a la plataforma de antivirus.
- Documento que indique la fecha de activación de 500 licencias y soporte técnico.

Los mencionados entregables deberán ser presentados por el contratista a través de la Mesa de partes (Presencial o Virtual) de la SUNASS, sito en Av. Bernardo Monteagudo 210 Magdalena del Mar, con Atención a la Unidad de Abastecimiento. Mesa de partes virtual <http://notificaciones.sunass.gob.pe:8080/mesadepartes/inicio-general>.

13. PARA LA FIRMA DEL CONTRATO

El contratista deberá presentar lo siguiente:

- Documento que señale el número telefónico y correo electrónico, conforme a lo solicitado en el numeral 7 de los Términos de Referencia (Soporte Técnico).
- Documentos que acrediten contar con lo solicitado en el numeral 8 de los Términos de Referencia.
- Copia de los documentos que acrediten contar con las certificaciones solicitadas para el Personal Clave, conforme a lo detallado en el numeral 9 de los Términos de Referencia.

14. MODALIDAD DE EJECUCIÓN

No corresponde.

15. SISTEMA DE CONTRATACIÓN

Suma alzada.

16. SUPERVISIÓN Y CONFORMIDAD

- El control y seguimiento de las actividades que se desarrollarán en el marco del servicio contratado, estará a cargo de un Coordinador designado por el jefe de la Oficina de Tecnologías de Información de la SUNASS.

- SUNASS luego de la evaluación respectiva, podrá otorgar la conformidad a los entregables, en caso contrario comunicará al contratista, las observaciones que considere, otorgándole un plazo para subsanar de acuerdo a la normativa vigente sobre contrataciones.
- La conformidad de los entregables, será emitida por el jefe de la Oficina de Tecnologías, de información de la SUNASS, a través de un informe técnico previo, emitido por el coordinador designado por la Oficina de Tecnologías de Información y firmas de las Actas respectivas.
- La conformidad será otorgada de acuerdo al Artículo 168 del reglamento de la ley de contrataciones del estado, por el Jefe de la Oficina de Tecnologías de Información, luego de verificado el cumplimiento de las condiciones contractuales.

17. FORMA DE PAGO

La Sunass realizará el pago de la contraprestación pactada a favor del contratista en soles y en dos (02) armadas de acuerdo con la TABLA N° 02, y según lo señalado en el artículo N° 171 del Reglamento de la Ley de Contrataciones del Estado, luego de la emisión del Acta de Conformidad por parte del jefe de la Oficina de Tecnologías de la Información.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Entregable según lo señalado en el Numeral 12 de los Términos de Referencia.
- Comprobante de pago.
- Acta de conformidad del jefe de la Oficina de Tecnologías de la Información-OTI.

TABLA N°02

Grupos	Forma de pago
1er Grupo (500 suscripción de licencias y soporte técnico)	50% del monto total del contrato
2do grupo (500 suscripción de licencias y soporte técnico)	50% del monto total del contrato

18. PENALIDADES APLICABLES

De acuerdo con lo establecido en el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

19. RESPONSABILIDADES POR VICIOS OCULTOS

El plazo de responsabilidad del contratista por la calidad ofrecida y por los vicios ocultos del servicio ofertado es de un (01) año contado a partir de la conformidad otorgada.

20. CLAUSULA ANTISOBORNO

- El contratista declara conocer los compromisos antisoborno de la SUNASS, el cual se establece en su Política antisoborno y se encuentra disponible en el portal web de la SUNASS (<https://cdn.www.gob.pe/uploads/document/file/4573329/Politica%20del%20SIG%202023.pdf?v=1684366588>)*
- El contratista declara no haber, directa o indirectamente, ofrecido, negociado o efectuado pago o, en general, entregado beneficio o incentivo ilegal en relación al servicio a prestarse o bien a proporcionarse. En línea con ello, se compromete a actuar en todo momento con integridad, a abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio, percibido de manera directa o indirecta; a cualquier miembro del Consejo Directivo, funcionarios públicos, empleados de confianza, servidores públicos; así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor*

estimado, elaboración de documentos del procedimiento de selección, calificación y evaluación de oferta, y la conformidad de los contratos derivados de dicho procedimiento.

- c. El contratista se compromete a denunciar, sobre la base de una creencia razonable o de buena fe, cualquier intento de soborno, supuesto o real, que tuviera conocimiento a través del canal de denuncias de soborno ubicado en el portal web de la SUNASS (<http://servicio.sunass.gob.pe/denuncias/>)

21. CLÁUSULA ANTICORRUPCIÓN

El/la proveedor/a declara y garantiza no haber ofrecido, negociado o efectuado, cualquier pago o; en general, cualquier beneficio o incentivo ilegal en relación con la orden de servicio o el contrato, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios/as, integrantes de los órganos de administración, apoderados/as, representantes legales, funcionarios/as, asesores/as o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Asimismo, el/la proveedor/a se obliga a conducirse en todo momento, durante la ejecución de la orden de servicio o 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/as, accionistas, participacionistas, integrantes de los órganos de administración, apoderados/as, representantes legales, funcionarios/as, asesores/as y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado. Además, el/la proveedor/a se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

El incumplimiento de las obligaciones establecidas en esta cláusula faculta a SUNASS a resolver automáticamente y de pleno derecho la orden de servicio o el contrato, bastando para tal efecto remitir a EL CONTRATISTA una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiera lugar.

22. CONFIDENCIALIDAD

El contratista deberá mantener estricta confidencialidad sobre la información a la que tendrá acceso durante la ejecución del servicio. Asimismo, no podrá disponer de ésta para fines distintos al servicio que presta.

El contratista deberá de tener conocimiento de las “Disposiciones de seguridad de la información para proveedores” que serán comunicadas por la SUNASS si por la contratación el proveedor tiene acceso a algún activo de información de la SUNASS (sistemas de información, instalaciones de procesamiento, entre otros).

El contratista deberá de enviar al correo electrónico del personal responsable de la contratación del servicio la declaración jurada de compromiso de confidencialidad de proveedores de la Sunass firmada. El proveedor podrá ser evaluado de acuerdo con los lineamientos de seguridad de la información.

23. REQUISITOS DE CALIFICACIÓN

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<u>Jefe De Proyecto (01)</u> <u>Requisitos:</u> Título profesional en Computación y/o Informática y/o Sistemas y/o Redes y/o Comunicaciones.

	<p><u>Acreditación:</u></p> <p>El Título será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p><u>Personal De Soporte (01)</u></p> <p><u>Requisitos:</u></p> <p>Título Técnico o Bachiller o Título profesional de las carreras de Informática y/o Computación y Sistemas y/o redes y/o comunicaciones o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Redes y Computación o Ingeniería de Sistemas.</p> <p><u>Acreditación:</u></p> <p>El Grado de bachiller o Título será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Grado de bachiller o Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p><u>Personal De Implementación (01)</u></p> <p><u>Requisitos:</u></p> <p>Título Técnico o Bachiller o Título profesional de las carreras de Informática y/o Computación y Sistemas y/o redes y/o comunicaciones y/o telecomunicaciones.</p> <p><u>Acreditación:</u></p> <p>El Título o grado de bachiller será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el Título o grado de bachiller no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	CAPACITACION
	<p><u>Personal De Soporte (01)</u></p> <p><u>Requisitos:</u></p>

	<p>Capacitación en ETHICAL HACKER V12 con participación mínima de cuarenta (40) horas lectivas de formación.</p> <p><u>Acreditación:</u> Se acreditará con copia simple del certificado o constancia que acredite lo requerido.</p> <div data-bbox="320 436 1399 580" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div> <p><u>Personal De Implementación (01)</u></p> <p><u>Requisitos:</u></p> <p>Capacitación en METODOLOGÍAS AGILES Y ENFOQUES LEAN, con una participación mínima de cuarenta (40) horas lectivas de formación.</p> <p><u>Acreditación:</u> Se acreditará con copia simple del certificado o constancia que acredite lo requerido.</p> <div data-bbox="320 920 1399 1064" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Jefe De Proyecto (01)</u></p> <p><u>Requisitos:</u></p> <p>Experiencia profesional mínima de tres (03) años como Jefe de Proyectos y/o Gestor de Proyectos de TI y/o Coordinador de Proyectos de implementación y/o mantenimiento de antivirus y/o, antispam y/o ciberseguridad.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p><u>Personal De Soporte (01)</u></p> <p><u>Requisitos:</u></p> <p>Experiencia mínima de tres (03) años como analista de procesos y/o gestión de soporte y/o mantenimiento de soluciones antivirus, y/o antispam y/o ciberseguridad.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p>

	<p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p><u>Personal De Implementación (01)</u></p> <p><u>Requisitos:</u></p> <p>Experiencia mínima de dos (02) años en implementación y/o mantenimiento de antivirus y/o soluciones de protección de endpoint y/o ciberseguridad.</p> <p>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento</i> • <i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> • <i>Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</i> </div>
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 160,000.00 (ciento sesenta mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 20,000.00 (Veinte mil con 00/100 soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la</p>

	<p>condición de micro y pequeña empresa. Se consideran servicios similares a los siguientes:</p> <p>Suscripción de Licencias de Antivirus y/o antispam y/o firewall y/o soluciones de ciberseguridad. Servicios de soporte y/o implementación de plataforma de seguridad.</p> <p>Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo Respectivo referido a la Experiencia del Postor en la Especialidad.</p>
--	---

¹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

“... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”

(...)

“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.