TERMINO DE REFERENCIA N° 00097-2026/SBN-OTI

SERVICIO SUSCRIPCIÓN DE LICENCIA DE SOFTWARE DE CONTROL DE ACCESO A RED

CENTRO DE COSTO	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
N° CMN	2806
ACTIVIDAD POI Y/O ACCIÓN ESTRATÉGICA PEI	C0024 – OTI.05 GESTIÓN DE LA CONTINUIDAD OPERATIVA DE LA PLATAFORMA TECNOLÓGICA DE LA SBN
FUENTE DE FINANCIAMIENTO	RECURSOS ORDINARIOS
META	20
CLASIFICADOR DE GASTO	2.3. 2 5. 1 99
DENOMINACIÓN DE LA CONTRATACIÓN	SERVICIO SUSCRIPCIÓN DE LICENCIA DE SOFTWARE DE CONTROL DE ACCESO A RED

1. ÁREA USUARIA:

Oficina de Tecnologías de la Información

2. FINALIDAD PÚBLICA:

El presente servicio tiene como finalidad garantizar la continuidad y operatividad del software de control de acceso a la red de la SBN, permitiendo un acceso seguro y autorizado a los recursos de la red institucional, tanto para el personal CAP y CAS que realiza teletrabajo y terceros que se conectan mediante VPN, como para los usuarios internos de las distintas sedes de la Entidad. Todo ello bajo un enfoque de confianza cero, que permita verificar y controlar los accesos a la red, reducir el riesgo de accesos no autorizados y fortalecer la seguridad de la infraestructura tecnológica institucional. De esta manera, se contribuye a la continuidad de las actividades institucionales y a la adecuada atención de los administrados.

3. OBJETO DE LA CONTRATACIÓN:

Renovar la suscripción del software de control de acceso a la red, a fin de incorporar una capa adicional de seguridad para la protección de los recursos de la red mediante un enfoque de confianza cero, de modo que solo los usuarios y dispositivos verificados y autorizados puedan acceder, tanto desde el exterior como desde la red interna, a los recursos de la red de datos institucional, minimizando el riesgo de accesos no autorizados y mejorando la visibilidad y el control del tráfico de red.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

4. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

Antecedentes

La SBN, mediante Resolución N.°0046-2025/SBN-OAF (22/08/2025), aprobó la compatibilización del requerimiento para la adquisición de licencias/suscripciones de la marca Fortinet, destinadas a renovar el licenciamiento del equipamiento de ciberseguridad ya existente en la entidad (Fortigate, FortiAnalyzer, FortiManager, FortiClient-EMS). La aprobación tiene vigencia de 3 años, sujeta a que se mantengan las condiciones que la motivaron, y se sustenta en la Ley N° 32069 y la Directiva N.°0001-2025-EF/54.01.

Alcance del Servicio

El servicio comprende la renovación de la suscripción del software de control de acceso a la red para 700 dispositivos, incluyendo su activación, configuración, puesta en funcionamiento, actualizaciones, soporte técnico y capacitación. La solución deberá mantener compatibilidad e integración con la infraestructura tecnológica preexistente de la SBN.

El servicio de renovación suscripción de licencias de software de control de acceso a la red corresponde al siguiente producto:

Item	Producto	Tipo de Solución	Marca	Vencimiento de la suscripción vigente
01	Forticlient EMS (Licenciamiento para 700 endpoints)	Cloud	Fortinet	28/10/2026

Descripción del servicio

El servicio comprende la renovación de la suscripción del Software de Control de Acceso a la Red, conforme a los siguientes requerimientos:

Características Generales:

- Debe permitir la gestión centralizada del cliente de seguridad de endpoint desde una consola central provista por el fabricante desde la nube.
- El licenciamiento debe estar basado en la cantidad de clientes registrados en la consola de gestión central del mismo fabricante.
- Debe incluir licenciamiento para al menos 700 dispositivos durante el periodo de 1 año.
- Debe ser compatible al menos con los siguientes sistemas operativos: Microsoft Windows: 7 (32-bit and 64-bit), 8 (32 e 64 bits), 8.1 (32 e 64 bits) y 10 (32 e 64 bits); Microsoft Windows Server 2012 o posterior.
- Debe ser compatible con Linux Ubuntu 16.04 o posterior
- El cliente de seguridad debe tener interfaz gráfica de usuario al menos en el idioma

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

inglés y español.

- El cliente de seguridad debe poder generar bitácora (logs) sobre las funcionalidades instaladas y configuradas.
- Debe tener la capacidad de enviar alertas por correo.
- El fabricante debe proveer un portal para descargar el agente y permitir la instalación local.
- Debe ser compatible con la instalación vía Group Policy Object u otra herramienta provista por el postor.
- Debe tener la capacidad de generar un paquete de instalación que establezca la conexión con la consola de administración una vez desplegado.

Funcionalidades:

Filtrado de contenido Web

- Debe permitir la configuración de perfiles de filtro de web desde la consola central del mismo fabricante.
- Debe permitir la configuración de perfiles de filtro web basado en al menos 30 categorías predefinidas por el fabricante.
- El fabricante debe admitir consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc) para aplicar política de control de acceso a internet.
- El cliente de seguridad debe admitir reglas estáticas de acceso a internet basado en expresiones regulares.
- Para una URL determinada las acciones mínimas deben ser: permitir, bloquear, alertar o monitorear.
- Debe permitir desactivar el filtro web si detecta que el cliente se encuentra dentro de la red corporativa.

Escaneo de Vulnerabilidades

- El cliente de seguridad debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante.
- Debe permitir que el usuario comience un análisis de vulnerabilidades bajo demanda.
- Las vulnerabilidades encontradas deben brindar referencias de información desde una base de datos en internet. Debe incluir al menos: nombre, severidad y detalles.
- La consola central, debe permitir el parcheado automático de las vulnerabilidades detectadas en los endpoints cuando la aplicación con vulnerabilidad lo permita.
- El agente ZTNA debe tener funcionalidades de protección de endpoints y SASE. Las cuales podrán ser activadas con agregando la licencia respectiva.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

Funcionalidades de ZTNA

- El Agente, debe permitir crear una conexión cifrada segura hacia las aplicaciones protegidas sin usar VPN, conectándose con un ZTNA proxy provisto por el mismo fabricante o con el firewall perimetral de la organización.
- El agente en conjunto con los firewalls perimetrales existentes o el ZTNA proxy, deben permitir habilitar el acceso granular seguro a las aplicaciones sin importar si el usuario es local o remoto.
- La conexión debe permitir microsegmentación local
- La conexión cifrada deberá establecerse luego de verificar como mínimo, las credenciales del usuario y del dispositivo.
- Debe permitir verificar ciertas características del dispositivo remoto antes de permitirle acceder a los recursos de la organización. Debe validar al menos tres de las siguientes características: antivirus activo, firewall activo, vulnerabilidades, llaves de registro, equipo corporativo, grupo de dominio, dirección IP.
- Cada sesión se inicia con un túnel encriptado automático desde el agente hasta el proxy de ZTNA para la verificación del usuario y del dispositivo, Si se verifica, se otorga acceso para esa sesión.
- El agente debe soportar para ZTNA autenticación multifactor para proporcionar una capa adicional de seguridad.

VPN SSL

- Debe permitir que el usuario cree nuevas VPN SSL.
- Debe permitir que existan varias VPN SSL definidas simultáneamente.
- Debe permitir la personalización del puerto TCP en el que funciona la VPN SSL
- Debe permitir la autenticación usando usuario más clave y certificados digitales.
- Debe permitir la autenticación de dos factores provisto por el mismo fabricante.
- Debe permitir desplegar de manera centralizada, la configuración de VPN sobre los clientes de seguridad.

VPN IPSEC

- Debe permitir que el usuario cree nuevas VPN IPSEC.
- Debe permitir que existan varias VPN IPSEC definidas simultáneamente.
- Debe permitir la autenticación usando usuario más clave y certificados digitales.
- Debe permitir la selección de Modo Main y Agressive.
- Debe permitir el uso de NAT Traversal.
- Debe permitir la autenticación de dos factores provisto por el mismo fabricante.
-

Funcionalidades de la plataforma de gestión

- Debe permitir adicionar clientes mediante la adición de licencias.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

- Debe permitir la creación de usuarios de diferente perfil administrativo.
- Debe permitir configuración de diferentes grupos y perfiles para facilitar la administración.
- Debe permitir la configuración centralizada de perfiles de webfilter, scanner de vulnerabilidades y VPN.
- Debe permitir configurar la búsqueda vulnerabilidades de forma programada.
- Debe permitir configurar filtro de URL's provisto por el fabricante con al menos las siguientes acciones: bloquear, advertir, permitir y monitorear
- Debe permitir configurar filtro de URL's basado en wildcards o expresiones regulares con las siguientes acciones: bloquear o permitir
- Debe permitir configurar la conexión automática de VPN.
- El sistema de gestión central debe tener disponible información sobre: Cantidad de dispositivos gestionados, Versión de Sistema Operativo, Perfil aplicado, Usuario, etiquetas de confianza cero asignadas, estado del cliente de seguridad (Registrado o no registrado), Ubicación (dentro o fuera de la red), detalle de hardware del dispositivo.
- Capacidad de ejecutar reglas de etiquetado de confianza cero, a fin de asignar al endpoint dentro de un grupo dinámico automáticamente, de acuerdo con la verificación de uso de certificados, pertenencia a un dominio empresarial, versiones de OS, estado de vulnerabilidades, entre otros.
- Debe agrupar dinámicamente a los endpoints en función de la información que recibe de los agentes, utilizando las reglas de etiquetado de confianza cero configuradas.
- La consola central, se debe integrar con los firewalls perimetrales existentes en la red del cliente, permitiéndole esta integración, enviar a los firewalls información de todos los endpoints que cuentan con el agente instalado.
- La consola central debe enviar a los firewalls del mismo fabricante la siguiente información de los endpoints: perfil de usuario, avatar, Mac address, Versión de OS, versión de agente, UUID del agente, Etiqueta de confianza cero asignadas.

Soporte Técnico:

El soporte técnico se brindará en modalidad 24x7 durante la vigencia de la suscripción. Las solicitudes podrán realizarse mediante correo electrónico y línea telefónica.

Por cada solicitud el contratista deberá generar un número de ticket que permita efectuar su seguimiento. El tiempo de respuesta no será mayor de dos (02) horas, contado desde el registro de la solicitud. Asimismo, el contratista deberá proporcionar el procedimiento de atención y el cuadro de escalamiento correspondiente.

El contratista deberá precisar el procedimiento de atención, deberá indicar los correos electrónicos de su mesa de ayuda y el número 0800.

Capacitación:

El proveedor debe realizar la capacitación dirigida para tres (03) personas profesionales y/o técnicos de SBN, de cuatro (04) horas como mínimo respecto al uso del software, la transferencia de conocimiento se realizará de manera remota, los

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

horarios y cronograma serán previamente coordinados con el Jefatura de la Oficina de Tecnologías de la Información. La capacitación la podrá brindar el personal clave.

5. REQUISITOS DEL PROVEEDOR Y/O PERSONAL

5.1 Perfil del proveedor:

- Inscripción vigente en el RNP.
- Personal natural y/o jurídica que se encuentre activo y habido en el registro de la SUNAT.
- No contar con impedimentos para contratar con el estado.
- Suscribir los Anexos N° 06, 07, 08 y 09.
- Contar con autorización del fabricante para comercializar la marca y brindar los servicios requeridos.
  Nota: *Para acreditar este requerimiento se requiere presentar una carta del fabricante o copia simple siempre que el contenido permita verificar el cumplimiento de lo requerido.*

5.2 Experiencia del proveedor:

Requisito:
El postor deberá acreditar un monto facturado equivalente a S/ 50,000.00 (Cincuenta mil con 00/100 soles) como mínimo, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: suministro, renovación, actualización, suscripción, licenciamiento, implementación, configuración, soporte y/o mantenimiento de soluciones de software de seguridad informática, tales como:

- Control de acceso a la red (NAC) y/o gestión de control de acceso.
- Confianza cero (Zero Trust, ZTNA) y/o seguridad de red.
- Gestión centralizada de endpoints y de seguridad.
- Gestión de endpoints y/o gestión unificada de endpoints (UEM).
- Gestión Centralizada y Unificada de Endpoints (UEM, MDM, EMM)
- Detección y respuesta en endpoints (EDR, XDR, MDR).
- Protección de endpoints (antivirus, antimalware, EPP).
- Acceso Seguro y Red (ZTNA / SASE / SWG)
- Prevención de Pérdida de Datos (DLP) y Seguridad Perimetral / Red (NGFW, SASE, SWG).
- También se consideran servicios similares aquellos que, bajo otra denominación comercial, correspondan a soluciones de software de ciberseguridad con funcionalidades equivalentes a las descritas.

Acreditación:
La experiencia del postor en la especialidad se acredita con un máximo de veinte (20) contrataciones, mediante 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 constancia de depósito, nota de

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

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 pago[1], o comprobantes de retención electrónico emitido por SUNAT por la retención del IGV[2]. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[3], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de servicio con conformidad o constancia de prestación**.**

5.3 Capacidad técnica y profesional:

A. EXPERIENCIA DEL PERSONAL CLAVE:

Requisitos:

Un (01) Implementador

Requisitos:
El personal clave propuesto como Implementador deberá acreditar una experiencia mínima de tres (03) años en actividades de diseño, instalación, configuración, implementación y/o administración de equipos y/o soluciones de seguridad de redes, seguridad perimetral o infraestructura de ciberseguridad, en entidades públicas y/o privadas.

Acreditación:
La experiencia del personal propuesto 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.

B. Calificaciones del personal clave

B.1 Formación académica: Profesional Universitario o Profesional Técnico

Profesional Universitario

Requisitos:

Título profesional y/o grado de bachiller en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Computación y Sistemas, Ingeniería de Computación, Ingeniería de Redes y Comunicaciones, Ingeniería de Telecomunicaciones, Ingeniería Electrónica y/o Ingeniería Eléctrica, Ingeniería Mecatrónica, Ingeniería Industrial, Ciencias de la Computación, Seguridad Informática, Ciberseguridad, Redes y Comunicaciones, Computación e Informática y/o carreras afines, para el personal clave requerido como Implementador.

[1] El solo sello de cancelado en el comprobante de pago, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación fehaciente de la cancelación. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).
[2] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).
[3] Se entiende “privados” como aquellos que no son entidades contratantes.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

Profesional Técnico

Requisitos:
Título técnico profesional en las carreras de Redes y Comunicaciones, Administración de Redes y Comunicaciones, Telecomunicaciones, Telemática, Comunicaciones de Datos, Seguridad de Redes, Seguridad Informática, Ciberseguridad, Infraestructura de Redes y Comunicaciones, Administración de Redes y Servidores, Sistemas de Telecomunicaciones, Electrónica y Telecomunicaciones, Computación e Informática, Sistemas Informáticos y/o carreras afines, para el personal clave requerido como Implementador.

Acreditación:
Los evaluadores o la DEC, según corresponda, verifican los grados o títulos profesionales en el Registro Nacional de Grados Académicos y Títulos Profesionales 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 del Ministerio de Educación, a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/ según corresponda.

B.2 Capacitación del personal clave
Requisitos:
Capacitación mínima de treinta (30) horas lectivas y/o académicas en seguridad de redes y/o networking, del personal clave requerido como Implementador.

Acreditación:
Se acreditará con copia simple de constancias y/o certificados y/o diplomas u otros documentos que acrediten fehacientemente la capacitación requerida, debiendo permitir verificar la materia de capacitación y el número de horas exigido.

6. MODALIDAD DE PAGO

Suma alzada

7. LUGAR Y PLAZO DE EJECUCIÓN

7.1 Lugar

Los documentos correspondientes al servicio de suscripción de software de control de acceso a Red deberán ser entregados en forma digital mediante correos electrónicos: ztna@sbn.gob.pe, mzavaleta@sbn.gob.pe. y wquispe@sbn.gob.pe

La activación del licenciamiento se realiza en arquitectura Cloud, previa coordinación con la Oficina de Tecnologías de la Información ubicada en: Calle Chinchón N°890 – San Isidro

7.2 Plazo de ejecución

Plazo de Entrega de Actas, Activación y Capacitación

El plazo para la entrega de actas de licenciamiento de las suscripciones será de hasta siete (07) días calendario, contados a partir del día siguiente de notificada la orden de servicio al contratista.

La capacitación deberá realizarse dentro de un plazo máximo de cinco (5) días calendario,

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

contados a partir del día siguiente de notificada la orden de servicio, previa coordinación con el área usuaria.

Plazo de Suscripción y Soporte Técnico

El servicio de suscripción del software de control de acceso a la red y el soporte técnico del fabricante tendrán una vigencia de trescientos sesenta y cinco (365) días calendario.

8. ENTREGABLE

ENTREGABLES	PLAZO MÁXIMO DE ENTREGA
El contratista presentará un (01) entregable con los siguientes documentos: ✓ Informe de la implementación, adjuntando evidencias fotográficas de la activación de las licencias. ✓ Acta de capacitación ✓ Comprobante de pago.	Hasta cinco (5) días calendario, posteriores a la culminación del plazo de activación.

9. LUGAR DE PRESENTACIÓN DE LOS ENTREGABLES

El entregable debe ser presentado, a través de la mesa de parte virtual: https://mpv.sbn.gob.pe/ (el horario es las 24 horas, pero es preciso señalar que la documentación que ingresa por la mesa de partes virtual después de las 16:30 horas será derivada al día siguiente hábil.) y/o presencial (en el horario de 08:30 a 16:30 horas), dirigido a la Oficina de Tecnologías de la Información

10. CONFORMIDAD DEL SERVICIO

La conformidad de servicio estará a cargo del Jefe de la Oficina de Tecnologías de la Información, previo informe técnico de la implementación de las licencias por parte del Especialista en Redes PAD III.
Para la conformidad el contratista deberá emitir toda la documentación solicitada en el numeral 8.
Dicha conformidad se otorgará en un plazo que no exceda de los siete (07) días calendario, contados desde el día siguiente de recibido el entregable.

Asimismo, son aplicables las disposiciones correspondientes a la conformidad establecidas en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

11. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad, paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

La Entidad, realiza el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO, en moneda nacional, con depósito en cuenta interbancaria (CCI) del contratista. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad debe contar con la siguiente documentación:

- Confirmación de recepción de las actas de licenciamiento mediante el correo de ztna@sbn.gob.pe, wquispe@sbn.gob.pe y mzavaleta@sbn.gob.pe.
- Documento en el que conste la conformidad de la prestación efectuada suscrita por la Oficina de Tecnologías de la información
- Comprobante de pago.

12. PENALIDADES

12.1 Penalidad por Mora:

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

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde F tendrá el siguiente valor: F = 0.40

La penalidad se regula por lo dispuesto en los artículos 119 y 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

12.2 Otras Penalidades

N°	Supuestos de aplicación de penalidad	Forma de Cálculo	Procedimiento de verificación
1	Incumplimiento en el plazo de capacitación	2% de una UIT por cada día de retaso	Previo Informe del OTI que sustente el incumplimiento.

13. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

La información y material producido bajo los términos de este servicio, tales como escritos, medios magnéticos, digitales, y demás documentación generados por el servicio, pasará a propiedad de la SBN.

El contratista se comprometo a guardar reserva de la información privilegiada que conociera en el ejercicio de sus funciones, tareas y demás actividades como parte de la ejecución de la prestación, no revelando en forma oral, escrita, ni por cualquier otro medio, hechos, datos, procedimientos, documentación e información de acceso restringido (confidencial), a la que tuviera acceso a partir del inicio de las prestaciones relacionadas con el referido servicio, manteniendo la confidencialidad de la misma de manera permanente.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

En caso que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, la SBN está autorizado a iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcir del perjuicio, y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

14. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de la Superintendencia Nacional de Bienes Estatales 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.

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

15. CLÁUSULA DE CUMPLIMIENTO (LEY DE PREVENCIÓN Y MITIGACIÓN DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PÚBLICO, LEY N° 31564).

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. 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.

16. COMPROMISO ANTICORRUPCIÓN Y ANTISOBORNO:

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.

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

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.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

17. SOLUCIÓN DE CONTROVERSIAS.

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación, son resueltos mediante conciliación.

18. 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 con 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.

Firmado digitalmente por: FARJE HORNA Pedro Alberto FAU 20131057823 hard
Fecha: 26/10/2026 17:23:22-0500

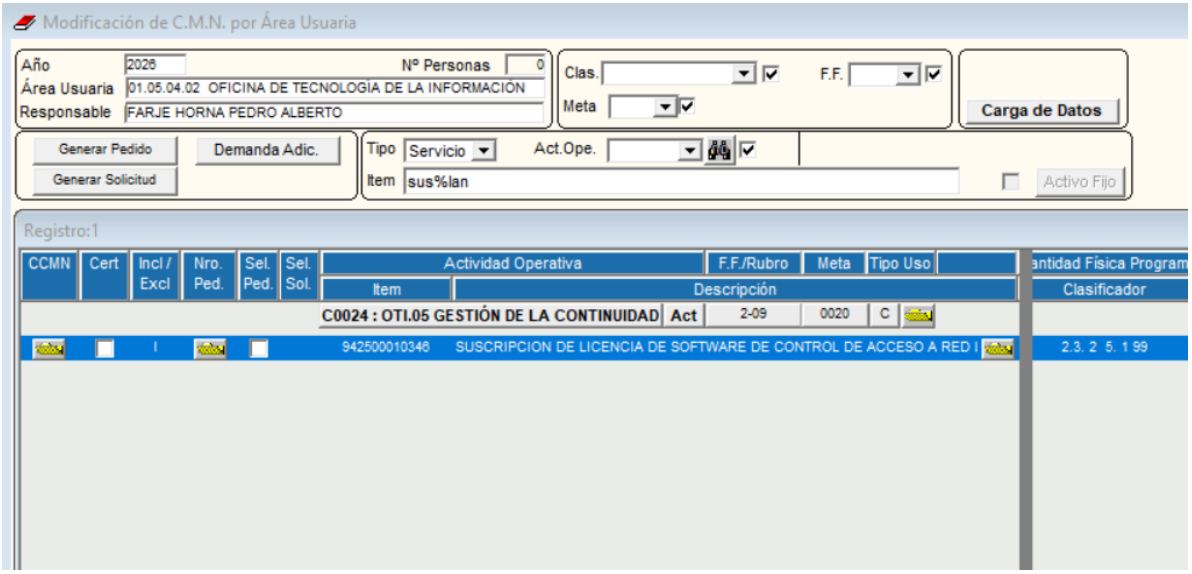
Firmado por:
PEDRO ALBERTO FARJE HORNA
Jefe
Oficina de Tecnologías de la Información

Firmado digitalmente por: QUISPE CHIPA William FAU 2013105782: hard
Fecha: 26/10/2026 17:22:45-0500

Firmado por:
WILLIAM QUISPE CHIPA
Especialista en Redes PAD III
Oficina de Tecnologías de la Información

Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1

SUSCRIPCION DE LICENCIA DE SOFTWARE DE CONTROL DE ACCESO A RED LAN



Esta es una copia auténtica imprimible de documento electrónico archivado en la Superintendencia Nacional de Bienes Estatales, aplicando lo dispuesto por el Art. 25 de DS.070-2013-PCM y la Tercera Disposición Complementaria Final del DS. 026-2016-PCM. Su autenticidad e integridad puede ser contrastada a través de nuestro portal web. https://www.sbn.gob.pe ingresando al ícono Verifica documento digital o también a través de la siguiente dirección web: https://app.sbn.gob.pe/verifica. En ambos casos deberás ingresar la siguiente clave:09832095U1