"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año de la Esperanza y el Fortalecimiento de la Democracia"

TERMINOS DE REFERENCIA PARA LA CONTRATACION DEL SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO, GARANTIA Y SOPORTE PARA LA SOLUCIÓN DE SEGURIDAD PERIMETRAL DEL FABRICANTE WATCHGUARD O EQUIVALENTE

1. AREA QUE REALIZA EL REQUERIMIENTO.

Oficina de Tecnología de Información

2. OBJETO DE LA CONTRATACION

Servicio de renovación del licenciamiento, Garantía y Soporte, de la solución de seguridad perimetral de la SUTRAN.

3. ACTIVIDAD VINCULADA AL POI

Con el presente servicio se podrá dar cumplimiento al Plan Operativo Institucional – POI del presente ejercicio en la actividad operativa Monitoreo e Implementación de Soluciones Tecnológicas de Sistemas Informáticos para la Entidad.

4. FINALIDAD PÚBLICA

La SUTRAN requiere contratar el Servicio de Licenciamiento, Garantía y Soporte de la solución de seguridad perimetral del fabricante Watchguard, a fin de mantener la seguridad informática de la plataforma de servidores de la SUTRAN en Lima.

5. OBJETIVO DE LA CONTRATACIÓN

- Objetivo General: Renovación de las funcionalidades de seguridad informática del equipamiento de seguridad perteneciente a la entidad.

- Objetivo Especifico: La SUTRAN requiere mantener las funciones de seguridad perimetral protegiendo de esta manera los aplicativos desplegados, así como de la infraestructura informática de servidores, minimizando con ello la materialización de ataques informáticos y accesos no autorizados.

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

En cumplimiento de las medidas de seguridad de la información establecidas en la entidad, se requiere la contratación del servicio de renovación del licenciamiento, garantía y soporte técnico para el equipamiento de seguridad perimetral del fabricante Watchguard actualmente instalado en la SUTRAN.

Para el presente servicio se tomó en consideración la aprobación de la estandarización de bienes y servicios de la Marca Watchguard aprobada mediante Resolución Jefatural N° D000150-2022-SUTRAN-OA.

Tabla N°1: Equipamiento actualmente instalado en la entidad.

Equipo	Modelo	Marca	Serie	Configuración
Firewall 01	M4600	Watchguard	80D602E16A8FB	Redundancia: Activo/ Espera Cubre las funcionalidades de Antispam, Firewall, IPS, filtro web, control de aplicaciones, antivirus, anti-APTs antispam, sistema de prevención de intrusos, control de aplicaciones, calidad de servicio, balanceo de enlaces, balanceo de carga, y Sistema de correlación de amenazas a nivel de redes y endpoints, entre otros.
Firewall 02	M4600	Watchguard	80D602E3BEFFA	

En esa línea, el servicio comprende lo siguiente:

• **Prestación principal**	Servicio de renovación del licenciamiento y garantía
• **Prestación accesoria**	Servicio de soporte técnico
	Capacitación

6.1 CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO (Prestación principal).

El contratista deberá renovar, por el periodo de un (01) año, el licenciamiento actualmente instalado en los equipos detallados en la Tabla N°1. Considerando que la licencia solo se colocará en el equipo que se encuentre en modo activo, si este fallase dicha licencia pasará al equipo en estado pasivo.

Tabla N°2: Características y condiciones del servicio principal

PRESTACIÓN	ITEM	DESCRIPCIÓN	CANTIDAD	Unidad de Medida
PRINCIPAL	**01**	Renovación de licenciamiento, garantía de la solución de Seguridad Perimetral del fabricante Watchguard.	01	Servicio.

A continuación, se describen las funcionalidades técnicas del licenciamiento a ser ofertado por el postor:

Manejo de VPN Ipsec

- ✓ Administración de certificados para construcción de VPNs cliente a sitio (client- to-site).
- ✓ Administración de VPN, para que solamente el usuario o la red que se conecte con una VPN especifica pueda ingresar a determinadas puertos, aplicaciones, y maquinas específicas de la Red LAN, protegida por el firewall.
- ✓ Soporte de VPN´s entre oficinas (Equipo – Equipo)
- ✓ El appliance deberá poder establecer túneles de VPN con cualquier otro producto de otra marca que tenga soporte de IPSec estándar.
- ✓ Soporte de VPN' s Móviles (Usuario – Equipo).
- ✓ El equipo debe soportar al menos 5000 VPN´s Móviles usando protocolo IPSec, si se requiere licenciamiento adicional este ya deberá estar incluido en la propuesta de la solución.
- ✓ Debe permitir VPN´s con clientes en S.O: Windows, Mac, Android y IOS
- ✓ Mecanismos de encriptación soportados DES, 3DES, AES 128-, 192-, 256-bit.
- ✓ Mecanismos de autenticación Ipsec soportados SHA-2, IKE v1/v2, IKE Pre- Shared Key, 3rd PartyCert
- ✓ Dead Peer Detection (DPD): Disponer de la funcionalidad de detectar el peer remoto cuando no es alcanzable falle o esté inoperativo
- ✓ Soporte para VPN Failover (re-establecimiento de la VPN sobre el segundo enlace en caso de fallas del enlace principal).
- ✓ Debe soporta VPN C2S (cliente a sitio) del tipo: IKEv2, L2TP, SSL y IPSEC, todos estos tipos de vpn deben ser configurados desde la interface web de manera sencilla.

Antivirus, Antispyware y Anti-rasonware a nivel perimetral.

- ✓ Analizar en tiempo real tráfico HTTP, HTTPS, FTP, SMTP, IMAP, POP3.
- ✓ La administración de antivirus en tiempo real, debe estar integrado a la plataforma de seguridad "appliance".
- ✓ El antivirus debe tanto ejecutarse usando firmas de detección, así como escaneo basado en comportamiento para poder capturar virus polimórficos y código malicioso.

- ✓ Administración de antivirus para filtrar archivos por extensión o por tipo de archivo MIME.
- ✓ Administración de antivirus y detención de tráfico spyware, adware y otros tipos de malware.
- ✓ Administración de actualizaciones tanto de motores como de definiciones de virus.
- ✓ El administrador del firewall debe ser capaz de elegir que escanear y que acción tomar cuando malware es detectado, incluyendo opciones de permitir, bloquear, hacer drop o mandar a cuarentena.
- ✓ La interfaz debe permitir elegir al administrador que acción tomar cuando ocurren algunas de las siguientes acciones:
  - Cuando un error de escaneo ocurre
  - Cuando el tamaño del archivo excede el máximo permitido.
  - Cuando el contenido es encriptado o protegido por contraseña.
  - El antivirus debe ser capaz de revisar archivos comprimidos como rar, tar, bzip2 y zip.
- ✓ Este licenciamiento deberá permitir que el equipo tenga un servicio de reputación basado en nube para clasificar la página web y de esa manera poder emitir un veredicto antes de que se haga el análisis antivirus y de esa manera no ocasionar un delay no deseado en la comunicación web. El tráfico a URLs con mala reputación debe ser inmediatamente bloqueado.
- ✓ Este servicio de reputación debe detectar conexiones desde y hacia nodos botnet.
- ✓ La renovación del licenciamiento permitirá que el producto incluya una opción de sandboxing, que permita la protección contra ransomware, amenazas de día cero y nuevos tipos de malware.
- ✓ Esta opción de sandboxing debe permitir al administrador realizar acciones como permitir, bloquear, hacer drop o mandar a cuarentena de acuerdo al nivel de amenaza. Este componente debe poder escanear al menos los siguientes tipos de archivos: docx, pptx, xlsx, pdf, apk, exe, dmg, rtf, txt, entre otros.
- ✓ Las definiciones de virus deben poder ser actualizadas y garantizadas durante el periodo de licenciamiento del producto.

Protección anti-Phishing

- ✓ La renovación de este licenciamiento permitirá que el producto pueda supervisar todas las solicitudes que pasan a través del equipo para evitar la conexión a dominios maliciosos.
- ✓ Esta capa de ser capaz de proteger de manera automática a los usuarios finales de ataques tipo pishing.
- ✓ La renovación de este licenciamiento deberá permitir que el producto brinde información detallada del ataque.

Sistema de Filtro Web

- ✓ Debe ser posible restringir o permitir URLs y categorías por usuario, grupo y de acuerdo a una programación horaria.
- ✓ Debe permitir el envío de notificaciones automáticas cuando un usuario trate de ingresar a un contenido boqueado.
- ✓ Administración de diferentes perfiles de utilización de la web (permisos diferentes por categorías) dependiendo de la IP, usuario o grupo de usuarios de donde inicie la conexión.
- ✓ Administración de reglas por usuarios locales (dentro del firewall) o externos (AD, LDAP, etc.).
- ✓ El filtrado web deberá incluir la opción de Filtrado por Categorías y subcategorías tanto sobre HTTP como HTTPS.
- ✓ Esta renovación de licenciamiento deberá permitir que el producto contenga al menos 80 categorías.

- ✓ Actualización automática de URLs en sus respectivas categorías.

Sistema de Prevencion de Intrusos (IPS)

- ✓ El sistema de prevención de intrusos debe hacer una inspección Deep-packet inspection a través de todos los puertos y protocolos. Debe captar, detectar y bloquear ataques por Anomalías (Anomaly detection) además de firmas (signature based/misuse detection).
- ✓ El sistema de detección de intrusos debe mitigar los efectos de los ataques de negación de servicios.
- ✓ Debe contar con los siguientes mecanismos de detección de ataques:
  - Reconocimiento de firmas, análisis de protocolos
  - Comparación contra normas RFC, para detección de anomalías.
  - Detección de anomalías
  - Detección de ataques de RPC
  - Protección contra ataques de Windows o NetBIOS
  - Protección contra ataques SMTP, IMAP, POP
  - Protección contra ataques DNS
  - Protección contra ataques FTP, SSH, Telnet.
  - Protección contra ataques de ICMP
  - Protección contra Gusanos y Virus, Exploits, Backdoor, DoS, Bots
  - Ataques tipo DoS
  - Puertas traseras (Backdoors)
  - Escaneo de Puertos (Port Scans)
  - Malware (gusanos, caballos de troya, rootkits, código malicioso móvil)
  - Pruebas de reconocimiento de la red
  - Ataques VoIP
  - Desbordamiento de búfer
  - Amenazas de día cero
- ✓ La administración del IPS debe ser por reglas, y no por interface, para evitar la carga y el delay innecesario y la revisión no apropiada del tráfico de red.
- ✓ Debe ser posible el bloqueo automático de direcciones ip que ejecutan ataques, por un tiempo especificado por el administrador.
- ✓ Debe ser posible crear excepciones de firmas de IPS y de direcciones IP.
- ✓ Notificación: Alarmas mostradas en la consola de administración del appliance y alertas vía correo electrónico.
- ✓ Actualización automática de firmas IPS.

Control de aplicaciones

- ✓ Deberá contar con más de 1,100 aplicaciones, organizadas por categorías.
- ✓ Debe poder administrar aplicaciones como Proxys Anónimos, Bases de Datos, CRMs, Photo y Video Sharing, Gaming, Herramientas de control remoto, P2P, mensajería Instantánea, entre otros.
- ✓ Deberá permitir, bloquear o restringir aplicaciones, incluyendo sub-funciones dentro de las propias aplicaciones.
- ✓ Debe ser posible controlar el ancho de banda que usan las aplicaciones, limitándolo con valores máximos y mínimos de trabajo.
- ✓ Debe ser posible visualizar desde el dashboard del equipo las aplicaciones que más consumen ancho de banda, y debe ser posible bloquear desde aquí las conexiones.
- ✓ Actualizaciones automáticas para incluir nuevas aplicaciones.

Protección Antispam

- ✓ Deberá detectar ataques de spam en cuanto ellos emergen para una protección inmediata y continua.

- ✓ El antispam debe poder crear listas blancas y negras por remitente o destinatario.
- ✓ El antispam debe ser capaz de etiquetar correo considerado como: Spam, probable Spam o Bulk.
- ✓ Deberá poder detectar y bloquear el spam, independiente del lenguaje, formato o contenido del mensaje.
- ✓ Deberá garantizar un porcentaje de falsos positivos cercano a cero.
- ✓ Deberá contar con una cuarentena para el almacenamiento de spam.
- ✓ El antispam debe trabajar a nivel de SMTP, POP3 e IMAP.
- ✓ Deberá contar con protección anti-relay.
- ✓ Las firmas de spam deben actualizarse regularmente, durante todo el periodo de renovación de licenciamiento del contrato del producto.

Sistema de correlación de amenazas a nivel de redes y endpoints

- ✓ Deberá tener una opción, basada en nube que permita correlacionar los eventos que ocurran en la red y a nivel del cliente (mediante un agente) para poder detectar, priorizar y permitir una acción inmediata contra ataques de malware.
- ✓ Deberá brindar una protección contra amenazas avanzadas (evasivas) y debe poder de manera automática intervenir para mandar a cuarentena, matar un proceso o borrar una llave de registro.
- ✓ Esta solución debe contar con un agente ligero a nivel de host que continuamente este monitoreando y enviando datos heurísticos y de comportamiento hacia la nube del producto para correlación y evaluación de los datos.
- ✓ Deberá contar con un módulo especifico anti-ransomware con tecnologías de análisis de comportamiento y honeypots para buscar signos de ransomware y automáticamente intervenir para detener la infección antes de que los archivos se pierdan.
- ✓ Deberá ser capaz de enviar alertas y notificaciones para permitir al administrador saber cuándo una amenaza o un incidente ha sido detectado, como también informar si la amenaza ha sido remediada a nivel de red o de endpoint.
- ✓ Deberá venir al menos con 200 sensores para las estaciones de trabajo.
- ✓ El sensor debe poder instalarse sobre los siguientes sistemas operativos:
  - Windows 8,10,11
  - Windows Server 2008,2012,2016,2019
  - Linux Red Hat / Centos 6,7,8
  - Mac OS 10.10,10.11,10,12,10,13
- ✓ Este servicio debe estar disponible y actualizable durante el tiempo de contrato del nuevo licenciamiento del firewall.

Consola de gestión centralizada.

- ✓ Debe incluirse una consola para la administración unificada de políticas de firewall, VPN, IPS, Antivirus, Control de Aplicaciones, Filtro de Contenido Web, Administración de ancho de banda, y antispam.
- ✓ La conexión entre el firewall y la consola deben ser cifrados.
- ✓ La consola debe proveer granularidad de reportes de cada módulo operativo de firewall, VPN, IPS, Antivirus, Control de Aplicaciones y Filtro de Contenido Web.
- ✓ La consola de administración debe permitir la creación de políticas offline.
- ✓ La consola debe mostrar información sobre la utilización de la red Internet (ancho de banda, aplicaciones, conexiones, entre otros)
- ✓ La consola de administración debe tener reportes gráficos en tiempo real que indique los parámetros de operación de una regla de ancho de banda (máximos y mínimos) para que esa manera sea más fácil poder afinar la regla.
- ✓ La consola debe permitir la visualización de eventos de seguridad en tiempo real.

Reportes (Watchguard Dimension)

- ✓ La renovación del licenciamiento debe incluir un appliance de reportes (físico o virtual) cuyo costo debe estar incluido en su propuesta. Este appliance debe recolectar los logs del firewall para poder generar reportes estadísticos e históricos de los eventos. En caso de ser virtual el appliance deberá ser compatible con VMware o Hyper-V.
- ✓ El contenido de los reportes debe incluir los datos en forma tabular (tablas) y/o gráficos, entre otros.
- ✓ La herramienta debe poder generar reportes programados.
- ✓ Debe tener reportes de salud del equipo, de CPU, Memoria, e inconvenientes con las interfaces físicas.
- ✓ La herramienta debe contener más de 40 reportes y dashboards.
- ✓ La herramienta debe contener reportes especiales de cumplimiento de normas como PCI y HIPAA
- ✓ Reporte Solución de Seguridad Firewall de Nueva Generación - Sistema de Protección Perimetral Integral de Tipo Appliance.
    - Información sobre la utilización de la red Internet (ancho de banda, aplicaciones, conexiones, entre otros)
    - Información integrada de servicios y acceso de Internet de los usuarios, IPs y nombre de PCs.
    - Información sobre el uso de las reglas creadas en el firewall.
    - Información sobre las páginas más visitadas y o categorías de URLs visitadas con mayor frecuencia, por fuente y/o destino.
    - Información de los accesos por usuarios a las VPNs activas.
    - Información de los ataques detectados/detenidos con mayor frecuencia en la red por fuente y/o destino.
    - Deberá permitir al administrador generar reportes en tiempo real, filtrándolas por aplicación y por enlace.
    - Acceso a categorías de páginas como entretenimiento, compras, y páginas de chat entre otras.
    - Los usuarios más activos en la red.
    - Los dominios web más visitados.
    - Información sobre el ranking de correos Spam, Dominios, Falsos Positivos detectados.
    - Estadísticas de efectividad de las reglas de filtrado de contenido creadas por el administrador.
    - Estadísticas de bloqueo de correo SPAM.
    - Estadísticas de bloqueo de virus y de amenazas avanzadas.
    - Informe del estado de los correos: entregados, bloqueados, cuarentena y rechazados como mínimo.
    - Los reportes deben ser exportables en formato HTML y PDF.
    - Desde esta herramienta de reportes debe ser posible ejecutar acciones urgentes, como bloqueo de clientes y dominios.
    - Esta consola de reportes también debe brindar la facilidad de ser el caso, de poder hacer un rollback hacia una configuración anterior del firewall.

Garantía del Hardware.

- ✓ Como parte de la renovación del licenciamiento se deberá considerar la garantía del Hardware emitida por el fabricante del equipamiento mencionado en la tabla N°1 del presente documento.
- ✓ La garantía del Hardware emitida por el fabricante deberá de considerar el reemplazo de los equipos o componentes de los equipos de seguridad perimetral que pudieran presentar fallas durante la ejecución del servicio.

6.2 PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL.

6.2.1. Capacitación

- El postor dará una capacitación técnica sobre el funcionamiento de los equipos de seguridad listados en la Tabla N°1 por un periodo de doce (12) horas como mínimo.
- La capacitación será brindada para un total de cuatro (04) personas como mínimo.
- La capacitación podrá brindarse se manera presencial o virtual, la misma que deberá de ser coordinada con la Oficina de Tecnología de Información (OTI).
- El contenido de la capacitación deberá desarrollar como mínimo los siguientes temas:

  - Gestión, administración y configuración del dispositivo.
  - Configuración de usuarios.
  - Configuración de Red WAN/ LAN/ DMZ.
  - Configuración de enrutamiento.
  - Sincronización con directorio activo.
  - Registro de eventos y monitoreo.
  - Políticas de Firewall.
  - Autenticación.
  - VPN SSL e IPSec.
  - Antivirus.
  - AntiSpam.
  - Filtro Web.
  - Perfiles de navegación.
  - Control de Aplicaciones.
  - Proxy Reverso.
  - Alta Disponibilidad.

- El personal a realizar la capacitación deberá de contar con la certificación técnica vigente de Trainer autorizado y/o Network Security Technical emitido por el fabricante Watchguard

6.2.2. Soporte Técnico de contratista.

- El Contratista deberá proporcionar el soporte técnico 24x7 ante cualquier incidencia y/o avería que pudiera presentarse en los equipos de seguridad.
- El soporte técnico podrá ser brindado a través de medios telefónicos, remoto y/o onsite.
- El tiempo del servicio de soporte técnico con el Contratista será por el período de trescientos sesenta y cinco (365) días calendarios contabilizados desde la activación de las licencias solicitadas en el punto 6.1 del presente documento.
- Para la firma del contrato, el contratista deberá indicar los números telefónicos de atención y correos de su centro de soporte técnico, así como los niveles de escalamiento para reportar un incidente técnico.
- La SUTRAN podrá reportar un incidente técnico ya sea de manera telefónica o por correo electrónico al centro de soporte técnico. El Centro de soporte técnico deberá de proporcionar un código de atención, que debe registrar la fecha y hora de registro del incidente para el posterior seguimiento de la misma.

- Para el caso de incidentes, la atención podrá realizarse de manera remota, salvo que previamente y por mutuo acuerdo entre el personal técnico de ambas partes, se convenga que dicho soporte sea en sitio.
- No debe existir límites de intervenciones ni de repuestos para corregir un desperfecto y retornar a los equipos a su estado operativo.
- El tiempo de espera de atención de un incidente no deberá ser mayor a cuatro (4) horas, entiéndase al tiempo transcurrido desde que se reporta un incidente o avería, hasta que el centro de soporte del Contratista asigna el código de atención.
- El Contratista tiene un plazo máximo de siete (07) horas luego de la asignación del código de atención para realizar el diagnóstico del incidente, luego del cual se realizarán las coordinaciones con la Oficina de Tecnología de la Información (OTI) para agendar la fecha y horario para realizar los cambios lógicos o de configuración necesarios, o de corresponder realizar los procedimientos de cambio de hardware por falla.
- El Contratista tiene un plazo máximo de doce (12) horas para la solución de incidentes técnicos, los cuales serán contabilizados desde el diagnóstico del incidente.
- El soporte técnico debe incluir actualizaciones de firmware y sistema operativo de los equipos listados en la Tabla N°1, así como la revisión y adecuación de las políticas de seguridad configuradas, a fin de garantizar el correcto funcionamiento de los mismos.

6.3 Documentación a presentar para la firma del contrato.

El postor deberá de presentar la siguiente documentación como parte de su oferta:

- El postor deberá acreditar mediante carta del fabricante (Watchguard) que está habilitado para la venta de equipamiento y licenciamiento de la marca.
- Para la firma del contrato, el contratista deberá indicar los números telefónicos de atención y correos de su centro de soporte técnico, así como los niveles de escalamiento para reportar un incidente técnico.
- Copia simple de la certificación técnica vigente del Trainer autorizado y/o Network Security Technical emitido por el fabricante Watchguard

6.4 Requerimientos del proveedor y de su personal.

6.4.1. Perfil del proveedor.

- Contar con RUC activo y Habido.
- Contar con Registro Nacional de Proveedores vigente.
- No contar con impedimento para contratar con el Estado.

6.4.2. Del personal del proveedor.

<u>Un (01) Especialista en seguridad perimetral</u>

Profesional o Técnico con experiencia certificada por la marca con más de 10 años (certificado por la marca).

Personal con Certificaciones como Auditor ISO 27001, Protección de Datos, ITIL, y similares.

Experiencia mínima de tres (03) años prestando servicios de instalación, configuración puesta en marcha, mantenimiento y soporte de equipamiento de seguridad perimetral de la marca Watchguard.

Actividades y funciones del especialista en seguridad informática

- Activación y configuración de las licencias a renovar.
- Acompañamiento en configuraciones, soporte, asesorías de la mano con el cliente.
- Reportes semanales, quincenales y mensuales.
- Revisión y Auditoria de la configuración trimestralmente.
- Adiestramiento y curso de la marca para 2 usuarios o administradores del equipo.
- Soporte 24x7
- Backup del archivo de configuración periódicamente o cambios relevantes.
- Asesorías de configuración para tener un mejor control y seguridad de la red.
- Alerta sobre conexiones peligrosa que puedan afectar a la red.
- Instalación y configuración de todos los servicios de seguridad del equipo.
- Actualización del sistema operativo del equipo.
- Monitoreo de la red para evaluar el funcionamiento.
- Asesorías de cualquier punto que requerido por el cliente.

7. PLAZO DE INSTALACION Y LICENCIAMIENTO DEL SERVICIO

La implementación del servicio deberá coincidir con la finalización de la licencia actual correspondiente al contrato N° 023-2025, la cual vence el 30 de julio de 2026.

Una vez culminada la instalación y Licenciamiento el contratista y la Oficina de Tecnología de la Información deberán suscribir un acta de instalación y licenciamiento del servicio. En caso surjan observaciones, estás deberán ser plasmadas en dicha acta, teniendo un plazo de tres (03) días calendario para absolver y/o resolver dichas observaciones.

8. ENTREGABLES POR EL SERVICIO

8.1 Entregables de la prestación principal.

- Cartas y/o documentos emitidos por el fabricante donde se detalle las características del licenciamiento ofertado, identificándose el periodo de renovación de las licencias referidas a la SUTRAN.
- Acta de instalación y activación del licenciamiento ofertado en el equipamiento de seguridad, acorde a lo indicado en el punto 6.1 del presente documento, el cual será suscrito por el jefe de la Oficina de Tecnología de Información y el representante del contratista.
-

8.2 Entregables de las prestaciones accesorias.

Capacitación:

- Acta de capacitación digital o impresa donde se detalle los participantes, así como la fecha y hora de la capacitación. Los lineamientos de la capacitación deberán alinearse a lo indicado en el numeral 6.3 del presente documento.
- Certificado digital o impreso dirigido a cada integrante de la capacitación.
- El Plazo de entrega será de diez (10) días calendarios, contabilizados a partir del día siguiente de la suscripción del contrato.

Soporte Técnico del contratista:

- Informes o reportes que permitan verificar el cumplimiento de los trabajos de soporte realizados acorde a lo indicado en el presente termino de referencia.

- El Plazo de entrega será de cinco (05) días calendarios, contabilizados a partir del día siguiente de la culminación del plazo de vigencia de la renovación de las licencias y garantía.

9. LUGAR DE PRESTACION DEL SERVICIO

El servicio se ejecutará en las instalaciones propias de la SUTRAN ubicada en la Av. Avenida Arenales Nº 452 Lima – Perú y/o fuera de SUTRAN.

10. PLAZO DE PRESTACION DE SERVICIO

10.1 Plazo de implementación y vigencia de la prestación principal.

- El plazo máximo de implementación del servicio de Renovación de licenciamiento y garantía de la solución de Seguridad Perimetral del fabricante deberá coincidir con la finalización de la licencia actual correspondiente al contrato N° 023-2025, la cual vence el 30 de julio de 2026.

- La renovación de las licencias y la garantía tendrá una vigencia de trecientos sesenta y cinco (365) días calendarios. El citado licenciamiento iniciará desde el vencimiento del actual licenciamiento instalado en la entidad.

10.2 Plazo de ejecución de la prestación accesoria.

Capacitación

- El plazo máximo para la ejecución de la capacitación será de diez (10) días calendarios contabilizados a partir del día siguiente de la suscripción del contrato.

Soporte Técnico.

- Plazo máximo de ejecución del soporte técnico será de trescientos sesenta y cinco (365) días calendarios, contabilizado a partir del día de la activación de las licencias y garantía.

11. FORMA DE PAGO

El pago se realizará en una sola armada, culminado el plazo de entrega y con el informe de evaluación técnico realizado por el personal especialista de OTI que verificará el cumplimiento de lo solicitado.

12. PENALIDAD

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. La penalidad se aplica automáticamente y se calcula de acuerdo al artículo 120 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas, conforme a la siguiente fórmula:

$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$	Donde F tiene los siguientes valores: Para bienes y servicios: F = 0.40

13. CONFORMIDAD

La conformidad será emitida por la Oficina de Tecnología de Información, dentro de un plazo hasta cinco (05) días hábiles, contados a partir del día siguiente de recepcionado el comprobante de pago respectivo del proveedor.

14. RESOLUCIÓN DEL 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 procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

15. 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 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. CONFIDENCIALIDAD

El proveedor guardará, bajo responsabilidad a que hubiere lugar, estricta confidencialidad respecto de la información a la que acceda para la realización de sus actividades, así como de la información que produzca, la cual es de propiedad de la SUTRAN. Queda prohibida la utilización de la información proporcionada para un fin distinto al contratado, así como expresamente se prohíbe su divulgación por cualquier medio.

17. ANTICORRUPCION

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, participacioncitas, 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.

18. GESTIÓN DE RIESGOS:

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

19. GARANTÍAS:

No corresponde.

20. SOLUCIÓN DE CONTROVERSIAS:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, conforme a lo establecido en Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas".