TERMINO DE REFERENCIA PARA EL SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO PARA EL EQUIPO DE SEGURIDAD PERIMETRAL DE LA SUTRAN

1. ÁREA USUARIA

Oficina de Tecnología de Información

2. OBJETO DE LA CONTRATACIÓN

Renovación del licenciamiento de dos (02) equipos de seguridad perimetral.

3. FINALIDAD PÚBLICA

Mantener la mejora en la Infraestructura Informática de la sede principal de la SUTRAN en Lima, así como la conectividad con sus Unidades Desconcentradas, renovando la solución de seguridad Perimetral, la cual permitirá el aseguramiento de la información digital de la SUTRAN

4. OBJETIVOS DE LA CONTRATACIÓN

Contar con la renovación del licenciamiento de dos (02) equipos de seguridad perimetral en la Sede principal de SUTRAN.

5. DESCRIPCIÓN DEL SERVICIO

La SUTRAN requiere mantener el endurecimiento a la seguridad perimetral de los servicios implementados, por lo cual se minimizará y prevendrá los ataques y accesos hacia la red informática, para ello se solicita:

ITEM	DESCRIPCION	CANTIDAD
01	Renovación Licenciamiento de 02 Equipos de Seguridad Perimetral.	02

5.1. Descripción detallada del bien existente del cual se requiere renovar el licenciamiento

El postor podrá presentar un nuevo equipamiento, acompañado del licenciamiento por un año, debiendo cumplir estas especificaciones mínimas:

Tipo	NGFW o UTM
Rendimiento de Firewall	36 Gbps
Sesiones concurrentes (TCP)	6 millones
Nuevas sesiones por segundo (TCP)	160,000
Políticas de Firewall	20,000 o superior
Rendimiento VPN/IPSec	8 Gbps
Túneles IPSec VPN Gateway a Gateway	2000
Túneles IPSec VPN Gateway a cliente	5000
Rendimiento IPS	5 Gbps
Rendimiento en Control de Aplicaciones	6 Gpbs
Rendimiento en protección contra las amenazas	6 Gbps o superior
VoIP	H.323, SIP
Balanceador de carga WAN	Si
Enrutamiento	Estático y Dinámico
Configuraciones de Alta Disponibilidad	Activo – Pasivo obligatorio, y

	Activo - Activo soportado.
Factor de Forma	Entre 1RU y 3RU
Tamaño	Entre 17" y 19", el equipo es rackeable.
Redundancia Eléctrica	El equipo cuenta con fuentes redundantes.
Cantidad de Interfaces 1Gbps (RJ45)	08
Puertos USB	02
Puerto Consola (RJ45)	01
Puerto de Administración (RJ45)	02
Ranuras SFP+ 10 GB	04 Incluye además 04 transceiver SFP+ y 04 cables LC-LC fibra de 5mts
Almacenamiento Interno	Tiene una capacidad de almacenamiento mayor a 120GB
Licenciamiento	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, DLP, y Sistema de correlación de amenazas a nivel de redes y endpoints, entre otros. El licenciamiento a renovar deberá ser por un periodo de 01 año adicional al vencimiento del actual. Considerar que la licencia solo se colocara en el equipo que se encuentre en modo activo, si este fallase dicha licencia pasara al equipo en estado pasivo.

5.2 Descripción detallada de aplicaciones soportadas por el nuevo licenciamiento

Manejo de VPN Ipsec

- ✓ Administración de certificados PKI X.509 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).
- ✓ El rendimiento de VPN debe ser de 8 Gbps al menos.
- ✓ Debe soporta VPN C2S (cliente a sitio) del tipo: 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.

Protección DLP

- ✓ La renovación de este licenciamiento permitirá que el producto incluya un componente DLP que permita proteger la información confidencial.
- ✓ Para facilitar la administración de esta característica, esta renovación de licenciamiento permitirá que el producto incluya una librería predefinida previamente cargada.
- ✓ Deberá trabajar a nivel de correo, web y FTP.
- ✓ Deberá poder revisar datos en más de 30 tipos de archivos, incluyendo PDF, Word, Excel, y PowerPoint.
- ✓ Deberá ser capaz de descomprimir archivos para extracción y revisión de los datos.
- ✓ Deberá ser capaz de crear reglas indicando el origen y el destino del contenido a enviar.
- ✓ El administrador debe poder definir la acción a tomar cuando la información confidencial es detectada por correo y por tráfico que no lo es.
- ✓ El administrador debe poder definir lo que ocurre ante errores de escaneo, información encriptada o protegida por contraseña.
- ✓ Entre las acciones disponibles deben figurar:
  - Permitir
  - Bloquear
  - Mandar a cuarentena.
  - Remover partes del mensaje.
- ✓ Actualización automática, durante el periodo de licenciamiento.

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 1,600 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
    - 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, DLP 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

- ✓ 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.

a) Consideraciones Generales

- En caso incluir un nuevo equipamiento, estos equipos componentes, partes, piezas, cables y accesorios deberán ser originales y nuevos del fabricante del equipo ofertado.
- El postor deberá acreditar mediante carta directa del fabricante que es habilitado para la venta de la marca ofrecida en el territorio del Perú.
- En caso que se incluya el nuevo equipamiento el proveedor deberá presentar una carta oficial emitida por el fabricante donde indique los equipos son nuevos.
- El postor, dentro del licenciamiento; deberá asegurar que los equipos estén protegidos ante fallas de hardware dentro del periodo del licenciamiento, estando debidamente asegurada con carta de fabricante.
- El postor deberá realizar un levantamiento de información previo para verificar la factibilidad de la implementación en caso incluya nuevo equipamiento, esta visita contará con un documento firmado por el responsable del proveedor y un representante de la SUTRAN. Este documento deberá ser adjuntado en la propuesta a presentar.

5.3 Actividades a Realizar

- Revisión y configuración de las actuales reglas de seguridad que tiene la solución.
- Creación de cuentas de administración del equipo de seguridad
- Registro de la garantía del equipo en el portal del fabricante a nombre de SUTRAN
- Configuración de Alta Disponibilidad de ambos equipos para el funcionamiento en Activo – Pasivo.
- Activación de las licencias adquiridas
- Creación y configuración de las políticas de seguridad del control de aplicaciones, filtro web, proxy reverso y demás componentes.
- Pruebas de funcionamiento y de Stress.
- Habilitará un total de veinticuatro (24) horas de soporte local o remoto ante el requerimiento de la entidad durante la vigencia del licenciamiento.

5.4 Capacitación

- El postor dará una capacitación igual o similar a la oficial, por un periodo de ocho (08) horas como mínimo para un total de cuatro (04) personas como máximo
- El contenido de las capacitaciones deberá tener como mínimo los siguientes temas:

  - ✓ Gestión, administración y configuración del dispositivo.
  - ✓ Registro de eventos y monitoreo
  - ✓ Políticas de Firewall
  - ✓ Autenticación
  - ✓ VPN SSL e IPSec
  - ✓ Antivirus
  - ✓ AntiSpam
  - ✓ Filtro Web
  - ✓ Control de Aplicaciones
  - ✓ Proxy Reverso
  - ✓ Alta Disponibilidad

- Las capacitaciones se realizaran máximo dentro de los cinco (05) días calendario siguientes de la configuración y activación de la licencia, previa coordinación con el área usuaria
- El postor dará un certificado de capacitación a cada uno de los participantes
- Las capacitaciones deberán ser impartidas por un personal técnico certificado de la marca que cumpla con los mismos requisitos del punto 6.B del presente documento.
- Este personal técnico deberá contar con un certificado adicional como personal autorizado en dictar entrenamientos autorizados por la marca a ofertar.

5.5 Recursos y Facilidades Provistos por la entidad

- Disponibilidad del personal TI para supervisión de las fases del proyecto.
- Coordinación con el equipo de TI que administra la seguridad perimetral para solicitar requerimientos técnicos necesarios.
- Acceso a los ambientes del Datacenter de la entidad**.**

5.6 Entregables

Una vez culminada la configuración y activación de la licencia, el contratista tendrá un plazo máximo de diez (10) días calendario para presentar la siguiente documentación:

- Certificados de capacitación emitidos por el postor.
- Informe técnico de las actividades realizadas correspondientes a la configuración de la renovación del licenciamiento del equipo de seguridad perimetral

Por otro lado, el Contratista deberá presentar el Certificado impreso de registro de renovación de licenciamiento

6. PERFIL DEL PERSONAL CLAVE

Personal técnico de la Implementación

- El personal debe contar con Certificación vigente como técnico en la solución a ofrecer o al tipo de licenciamiento a renovar, la cual deberá acreditar con copia simple de dicho certificado de la marca ofertada o a renovar y carta del fabricante confirmando la validez del certificado

7. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD TECNICA Y PROFESIONAL**
A.1	**CALIFICACIONES DEL PERSONAL CLAVE**
A.1.1	**FORMACIÓN ACADÉMICA**
	Personal técnico de la Implementación **Requisitos**: Titulado o bachiller en Ingeniería de Sistemas, Telecomunicaciones, Redes y Comunicaciones **Acreditación:** El grado o título profesional requerido 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 enlace: 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 enlace http://www.titulosinstitutos.pe/, según corresponda. En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerid
A.2	**EXPERIENCIA DEL PERSONAL CLAVE**
	Personal técnico de la Implementación **Requisitos:** Experiencia mínima de dos (02) años en la instalación, configuración y soporte de sistemas de seguridad perimetral y/o firewall en entidades públicas y/o privadas **Acreditación:** 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 que demuestren la experiencia del personal propuesto.

C	**EXPERIENCIA DEL POSTOR**
C.1	**FACTURACIÓN**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 80,000.00 (Ochenta 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. Se consideran servicios similares a los siguientes: - Servicio de renovación de licenciamiento de seguridad o firewall perimetral y/o

	servicio de soporte o mantenimiento de equipos de seguridad o firewall perimetral. **Acreditación:** Copia simple de contratos u órdenes de compra, y su respectiva conformidad por la venta o suministro efectuados; o comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con VOUCHER DE DEPÓSITO, REPORTE DE ESTADO DE CUENTA, CANCELACIÓN CON SELLO DE CLIENTE EN EL DOCUMENTO, ENTRE OTROS, correspondientes a un máximo de veinte (20) contrataciones. 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 Nº 7** referido a la Experiencia del Postor. En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N.º 7** referido a la Experiencia del Postor. **Importante** *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes ejecutan conjuntamente el objeto materia de la convocatoria, previamente ponder conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataci del Estado".*

8. PLAZO DE EJECUCION

El servicio se realizara por un plazo de máximo de siete (07) calendario acuerdo a lo siguiente:

- Configuración y activación del nuevo licenciamiento: Hasta cinco (05) días calendario, contabilizados a partir del día siguiente de suscrito el contrato, para lo cual suscribirán un Acta de configuración y activación en señal de conformidad.

- Actualización de la versión que corresponda: Hasta dos (02) días calendario a partir de la configuración y activación del nuevo licenciamiento

9. LUGAR DE PRESTACION

El postor deberá considerar que la configuración, activación y actualización de la solución ofertada se realizará en las instalaciones de OTI/SUTRAN, sito en el mezanine de la Av. Arenales 420, Jesús Maria.

10. GARANTIA COMERCIAL DEL BIEN

La garantía comercial del licenciamiento y/o equipamiento adquirido será de un (01) año como mínimo desde el vencimiento del equipo actual o desde la activación de un posible nuevo equipamiento.

11. FORMA DE PAGO

El pago se realizara en una sola armada, previa conformidad emitida por el área usuaria

12. CONFORMIDAD

La conformidad será entregada por la Oficina de Tecnología de Información, previa presentación de la documentación solicitada en el numeral 5.6

14. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y por los vicios ocultos por un plazo de un (01) año contado a partir de la conformidad otorgada por el área usuaria correspondiente.

13. PENALIDADES

Si el contratista incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplicará una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, en concordancia con el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

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

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F 0.40
b) Para plazos mayores a sesenta (60) días:
b.1) Para bienes, servicios en general y consultorías: F=0.25