PROCESO DE SELECCIÓN NIVEL 2 N° 001-2022 CMAC SANTA
"RENOVACION DE LICENCIAMIENTO PARA FIREWALL PERIMETRAL PA-820 POR EL PERIODO DE UN AÑO"

Chimbote, enero del 2022

ESPECIFICACIONES TECNICAS
REQUERIMIENTOS TÉCNICOS MÍNIMOS

I.-ITEM UNICO:

1. REQUERIMIENTOS GENERALES

Que la **CMAC SANTA SA** como entidad financiera líder en su rubro, cuente con la última versión disponible del microcódigo y soporte técnico de la solución tecnológica *Palo Alto*, para que siga protegiendo y administrando el tráfico de internet mediante el control de aplicaciones, filtro de URL, QoS, prevención de amenazas y VPN segura.

2. REQUERIMIENTOS FUNCIONALES

2.1. REQUERIMIENTOS ESPECÍFICOS.

La **CMAC Santa SA** cuenta con dos equipos Palo Alto (PA-820) configurados en HA con licencias en modo suscripción anual que deben ser renovadas antes de su caducidad.

La renovación, mantenimiento, soporte para las licencias y el equipo se mencionan a continuación.

DESCRIPCIÓN DEL PRODUCTO	CANTIDAD
DNS Security - Palo Alto Networks DNS Security License x 1 Año	2
Soporte Premium - 24 x 7 phone support; advanced replacement hardware Service x 1 Año	2
Threat Prevention x 1 Año	2
PAN-DB URL Filtering - Palo Alto Networks URL Filtering License	2
WildFire License - WildFire signature feed, integrated WildFire logs, WildFire API x 1 Año	2
Logging Service - Device Logging Service x 1 Año	2
Soporte de Servicios de Ingeniería para PA-820 con asistencia integral en Mesa de Ayuda 24x7x365 x 1 Año que incluye: Administración total del equipo de forma remota, soporte ilimitado de llamadas, control de cambios y soporte RMA con la marca Palo Alto.	1

La licencia deberá de ser registrado en los equipos mencionados.

En caso que el **PROVEEDOR** decida proponer un equipamiento totalmente nuevo, este deberá de ser de la misma marca *Palo Alto* y deberá de contemplar las siguientes características como mínimo a nivel de Hardware:

- Rendimiento de Cortafuegos: 3,8/3,2 Gbps
- Rendimiento de Prevención contra amenazas: 1,6/1,7 Gbps
- Rendimiento de VPN IPSec: 2,2 Gbps
- Número máximo de sesiones: 300,000
- Nuevas sesiones por segundo: 52,000
- Puertos RJ-45: 8 Puertos 10/100/1000 como mínimo.
- Puertos de Gestión: 1 Puerto de gestión fuera de banda.
- Capacidad de almacenamiento interno: 128 GB como mínimo.
- Número de equipos: 2 equipos físicos.
- Número de Fuentes por equipo: 2 fuentes redundantes por equipo.
- Rack-mount: Si, deberá de instalarse en el Gabinete de Comunicaciones.

El **PROVEEDOR** debe considerar la continuidad del servicio actual de protección de seguridad perimetral ofrecido por los equipos *PA-820* configurados en HA en todo momento. Entiéndase, que en el caso el **PROVEEDOR** opte por la opción de Renovación Tecnológica con equipos nuevo, deberá considerar renovar las licencias de los equipos actuales por el plazo necesario hasta que se realice la entrega de los nuevos equipos.

2.2. SERVICIOS REQUERIDOS

El **PROVEEDOR** deberá de cumplir con los siguientes entregables:

ENTREGABLE	PERIODICIDAD Y FECHA DE ENTREGA
Carta de entrega del servicio donde se especifique la vigencia de los componentes indicados en **Requerimientos Específicos.**	Una ocasión, a más tardar, 2 días hábiles posteriores al inicio de la vigencia del servicio.
Horarios y contacto para brindar el soporte técnico y datos de contacto para atenciones de emergencia, incluir el SLA.	Una ocasión, a más tardar, 2 días hábiles posteriores al inicio de la vigencia del servicio.
Reporte de ataques, caídas o disponibilidad del equipo, duración de incidentes, motivo, tickets abiertos, atención y cerrados.	**Mensual**, durante la vigencia del servicio. A más tardar a los 2 días hábiles posteriores al fin de cada mes hasta finalizar el contrato/servicio
Reporte SECURITY LIFECYCLE REVIEW (Reunión por MS Teams, Zoom u otro con el equipo de Infraestructura de la CMAC Santa y SOC del Proveedor).	**Trimestral**, durante la vigencia del servicio. A más tardar a los 2 días hábiles posteriores al fin de cada trimestre hasta finalizar el contrato/servicio

2.3. GESTIÓN DE RIESGO BASADO EN VULNERABILIDADES

- La CAJA definirá los 125 activos considerados como críticos para este servicio.
- La plataforma de gestión de vulnerabilidades debe encontrarse como líder en el último reporte "The Forrester Wave: Vulnerability Risk Management" de la Consultora Forrester o de algún similar.
- La solución propuesta debe realizar la validación de los parches y la revisión de seguridad.
- La solución debe admitir la implementación de análisis a través de agentes y / o motores de análisis específicos.
- La solución debe trabajar en un esquema híbrido, entre la red del cliente y la nube, para aquellos activos que se encuentren fuera de la red de la caja y que no cuenten con una conexión VPN hacia la caja.
- La comunicación de los agentes con la plataforma debe garantizar que los usuarios que se encuentren fuera de la oficina no tengan la necesidad de conectarse a la infraestructura de la empresa por medio de VPNs, así los agentes pueden conectarse directamente con la nube desde cualquier ubicación geográfica, sin la necesidad de rutas internas o de tener cualquier tipo de conexión con el entorno de la empresa.

2.4. GESTION DE MONITOREO Y DETECCION DE AMENAZAS

- El servicio de monitoreo y detección deberá permitir realizar escaneos constantes para validar la conectividad de los equipos y alertar en caso se registre una interrupción en la recepción de los eventos provenientes de los NGFW o deberá de permitir almacenar Logs constantes para respaldar la información de los equipos y alertar en caso se registre una interrupción en la recepción de los eventos provenientes de los NGFW.
- Permitirá la creación de filtros totalmente personalizados de los registros que provengan desde los NGFW.
- El proveedor soportará la cantidad total de eventos que provengan de los NGFW y de las subscripciones solicitadas.
- **Deberá contar con la capacidad para gestionar los eventos en línea de los últimos 30 días.**
- Las alertas e incidentes deberán de calificarse por su gravedad.
- El proveedor deberá alertar o comunicar a la caja de alguna anomalía o algún evento que detecte como sospechoso.
- El proveedor del servicio debe notificar a la caja sobre:
    - Alertas con reservas en las que se solicitan investigaciones internas para su confirmación.
    - Incidentes de seguridad confirmados que requieran tratamiento.

3. REQUERIMIENTOS NO FUNCIONALES

El **PROVEEDOR** deberá de presentar una carta de fabricante dirigida a **la CMAC SANTA SA** durante la etapa de presentación de ofertas donde se exprese que es un distribuidor autorizado y certificado de la marca *Palo Alto Networks.* Así mismo, deberá evidenciar que cuenta con el personal técnico

calificado y certificado (en planilla y no terceros) para proveer los servicios que la **CMAC SANTA SA** está solicitando.

El **PROVEEDOR** deberá de poseer como mínimo 2 personas con la certificación PCNSE, el cual deberá ser evidenciado en formato digital (PDF) y 2 personas con certificación técnica vigente en gestión de riesgo basado en las vulnerabilidades y gestión de monitoreo y detección de amenazas, lo cual deberá acreditar para la presentación de ofertas.

El **PROVEEDOR** deberá de evidenciar que cuenta con un SOC (Centros de Operaciones de Seguridad) y que es responsable directo (no terceros) de garantizar que se identifique, analice, mitigue y documente las incidencias de seguridad que pueda existir en nuestro equipo Palo Alto y la red de Internet.

Con el objetivo de mantener informado a la **CMAC SANTA SA**, el **PROVEEDOR** deberá de realizar los siguientes reportes de manera obligatoria:

REPORTE	PERIODO
Reporte de ataques, caídas o disponibilidad del equipo, duración de incidentes, motivo, tickets abiertos y cerrados y adicionales que considere necesario para la correcta gestión.	A mes vencido durante la vigencia del contrato.
Reporte SECURITY LIFECYCLE REVIEW (Reunión por MS Teams, Zoom u otro con el equipo de Infraestructura de la CMAC Santa y SOC del Proveedor).	Trimestral, durante la vigencia del servicio. A más tardar a los 2 días hábiles posteriores al fin de cada trimestre hasta finalizar el contrato/servicio

3.1. CARACTERISTICAS DEL PROVEEDOR

- Debe ser Partner certificado o asociado de negocio de la marca en la solución ofertada, para lo cual deberá adjuntar una carta del fabricante que así lo precise, este documento debe estar vigente a la fecha de la presentación de la propuesta, en donde también se precise que están autorizados a comercializar, implementar y dar soporte en la familia de productos ofertados.
- Debe acreditar una antigüedad no menor a tres (03) años en el mercado en actividades de informática o seguridad informática o similares, mediante la presentación en copia simple de la consulta ruc o ficha ruc emitida por la SUNAT y declaración jurada simple de los proyectos implementados y ejecutados, y se acreditará dicha experiencia con contratos u órdenes de compra o servicio y su respectiva conformidad del servicio.
- Deberá contar con SOC 24 x7 (Centro de Operaciones de Seguridad), a solicitud o demanda de CAJA SANTA, para lo cual deberá presentar la respectiva declaración jurada de cumplimiento.
- Debe contar con un Centro de Atención al cliente propio (help desk – mesa de ayuda) para el manejo de incidencias y/o las coordinaciones de soporte requeridas 24x7x365, así como generación de tickets de

atención, luego de la suscripción del contrato el postor ganador deberá entregar a CAJA SANTA el procedimiento de escalamiento correspondiente, así como el directorio telefónico, correos electrónicos y otros medios que permitan registrar los incidentes para su respectiva atención. En cumplimiento de esta viñeta, el postor deberá presentar el documento correspondiente que así lo acredite.

- Debe de contar con un número telefónico donde se pueda contactar con la mesa de ayuda las 24x7x365.
- Debe contar con un Centro de Operaciones de Seguridad (SOC) certificado en ISO 27001, lo cual deberá acreditar para la presentación de ofertas.
- Prestar el servicio desde un centro ubicado dentro del territorio peruano.
- Emitir con periodicidad mensual informes de seguimiento de los diferentes servicios objeto del contrato.
- Estar dotado de una estructura funcional con diferentes áreas operativas y niveles de especialización.
- Disponer de un sistema de etiquetera compatible y alineada con ITIL.
- Disponer de una línea gratuita 0800 a nivel nacional.
- Deberá de brindar un correo donde se reporten todos los incidentes y/o se hagan seguimiento.
- Deberá de permitir crear casos mediante los siguientes medios: llamada, correo.
- Deberá brindar un soporte y garantía de 12 meses.
- Deberá brindar el servicio de gestión del riesgo basado en las vulnerabilidades de 125 activos considerados como críticos para CAJA DEL SANTA. Asimismo, el **PROVEEDOR** deberá elaborar los objetivos de la CAJA basado en los riesgos identificados a través de las vulnerabilidades descubiertas. Por último, elaborar un plan de remediación teniendo como prioridad la reducción del riesgo identificado.
- El Postor deberá monitorear y detectar las principales amenazas avanzadas que constantemente los NGFW analizan, con la finalidad de alertarlos y contenerlos. Asimismo, el **PROVEEDOR** se encargará del despliegue todo el equipamiento y licenciamiento que se considere necesario para cumplir con el monitoreo inteligente de los mismos. El proveedor se responsabilizará del envío de eventos, el tipo de log que se deba enviar desde los equipos mencionados, la instalación/despliegue de sensores y/o dispositivos dentro de la red de la CAJA para cumplir con el monitoreo solicitado, alertar y contener las distintas amenazas que crucen la seguridad perimetral de la caja. El proveedor deberá incluir la arquitectura y el detalle del alcance del servicio de manera mandatorio dentro de su propuesta técnica.

4. **NIVELES DE SERVICIO.**

El **PROVEEDOR** se compromete a brindar soporte técnico y mesa de ayuda en 7x24x365, por el periodo de 1 año el cual incluye la administración total del equipo de forma remota, soporte telefónico ilimitado, control de cambios y equipo de remplazo en caso de falla grave. Acreditar con declaración Jurada.

Tiempo de respuesta: El tiempo de respuesta sugerido por la **CMAC SANTA SA** es el siguiente.

- Severidad 1 – Critica: < 1 Hora.
- Severidad 2 – Alto: 2 Horas.
- Severidad 3 – Medio: 4 Horas.
- Severidad 4 – Bajo: 8 Horas.

Tiempo de seguimiento: El tiempo de seguimiento esperado por la **CMAC SANTA SA** es el siguiente.

- Severidad 1 – Critica: Cada 2 horas hasta que se resuelva o se aplique un Workaround.
- Severidad 2 – Alta: Cada 24 Horas hasta que se resuelva o se aplique un Workaround.
- Severidad 3 – Medio: Cada 2 días laborales hasta que se resuelva.
- Severidad 4 – Bajo: Semanalmente hasta que se resuelva.

Definición de Severidad:

- Critica: El producto no funciona y afecta críticamente al entorno de producción. No existe Workaround disponible.
- Alta: El producto está deteriorado y el entorno de producción de cliente funciona con deficiencias. No existe Workaround disponible.
- Media: Una función del producto ha fallado y no se ve afectado el entorno de producción. El servicio de soporte lo conoce y existe un Workaround disponible.
- Baja: El funcionamiento del producto no se ve afectada y sin impacto en el negocio del cliente. Incluye información, documentación procedimiento y solicitudes de mejora por parte del **PROVEEDOR.**

5. **CRONOGRAMA DE ACTIVIDADES.**

El **PROVEEDOR** deberá de cumplir con el plan de trabajo previamente acordado con el personal técnico de la CMAC Santa SA, a través del Departamento de Tecnología de la Información.

El **PROVEEDOR** debe de realizar la actualización del Microcódigo del equipo hacia la última versión vigente, y deberá de evaluar la mejora al upgrade del Cliente VPN (GlobalProtect).

El **PROVEEDOR** deberá de presentar en su propuesta, un cronograma de actividades para la implementación y puesta en marcha de "**RENOVACIÓN DE LICENCIA PALO ALTO NETWORKS – CMAC SANTA SA**"**,** considerando que la fecha de inicio y fecha de fin no debe de impactar en la productividad de la **CMAC SANTA SA.**

6. **SEGUIMIENTO DEL SERVICIO.**

Con la finalidad de mantener informado a la **CMAC SANTA SA** sobre la **RENOVACIÓN DE LICENCIA PALO ALTO NETWORKS – CMAC SANTA SA**" el **PROVEEDOR** deberá de notificar por escrito o de manera electrónica cada vez que existe un UPGRADE al Software de equipo, así como a los componentes del mismo durante la vigencia del contrato, sin esperar a que la **CMAC SANTA SA** notifique o haga seguimiento.

7. **INFORMACIÓN ADICIONAL.**

El **PROVEEDOR** y la **CMAC SANTA SA** administrarán el equipo de manera compartida. La **CMAC SANTA SA** podrá realizar y ejecutar controles de cambios en el equipo sin afectar la disponibilidad de la misma.

El **PROVEEDOR** deberá de brindar un entrenamiento técnico constante para dos personas. Esto con la finalidad de poder realizar la administración compartida de manera eficiente. Esta capacitación se debe de realizar de la siguiente manera:

- Capacitación técnica al inicio de realizar el licenciamiento y explicar detalladamente el funcionamiento del equipo.
- Cualquier ticket de soporte abierto y solucionado por EL PROVEEDOR, este deberá de brindar una guía y una explicación por MS Teams, Zoom u otro medio conectado a la consola Web para tenerlo en cuenta en futuros escenarios.

II.-VALOR REFERENCIAL:

S/ 48,000.00 Soles (Cuarenta y ocho mil con 00/100 Soles) .

El Valor referencial incluye todos los tributos, seguros, transportes, inspecciones, costos laborales, conforme a la legislación vigente, así como cualquier otro costo que pueda tener incidencia sobre el costo del bien y/o servicio a contratar.

III.- CRONOGRAMA DEL PROCESO:

ETAPA	FECHA
Convocatoria	Del 26/01/2022
Presentación de Propuestas	31/01/2022
Evaluación, Calificación y Elección de la Propuesta Ganadora	01/02/2022
Buena Pro	01/02/2022

IV.-EVALUACIÓN DE PROVEEDORES:

Evaluación Técnica	Puntaje
Experiencia del Postor Experiencia comprobada en Seguridad Informática mínima de 3 Años, acreditando con contratos u órdenes de compra o servicios y sus respectivas constancias de conformidad de servicio,.	40
Tiempo de Generación de Licencia **Tiempo de Instalación** / **Puntaje** Hasta 15 días / 30 puntos Hasta 30 días / 20 puntos	30
(01) Examen + Curso ITIL 4 Fundamentos en Academia Autorizada (Online).	15
Certificaciones en ISO 9001 o ISO27001 o Seguridad Informática a nombre del **PROVEEDOR,** acreditando con copias de las certificaciones donde se pueda evidenciar el código de verificación.	15

Para pasar a la oferta económica el postor deberá alcanzar un puntaje mínimo de 70 puntos.

Evaluación Económica	$P_i = O_m \times 100 / O_i$
Consistirá en asignar el puntaje máximo establecido (100) a la propuesta económica de menor monto. Al resto de propuestas se les asignará un puntaje inversamente proporcional.	i = Propuesta P_i = Puntaje de la propuesta económica i O_i = Propuesta económica i O_m = Propuesta económica de monto/precio más bajo

PUNTAJE TOTAL:

Una vez calificadas las propuestas mediante la evaluación técnica y económica se determinará el puntaje total de las mismas.

El puntaje total de la propuesta será el promedio ponderado de ambas evaluaciones, obtenido de la siguiente fórmula:

PTPi = c1 PTi + c2 PEi

Donde:

PTPi = Costo Total del postor i
PTi = Puntaje de la evaluación técnica del postor i
PEi = Puntaje de la evaluación económica del postor i
c1 = Coeficiente de ponderación para la evaluación técnica = 0.60
c2 = Coeficiente de ponderación para la evaluación económica = 0.40

V.-PRESENTACION DE PROPUESTAS:

Las propuestas se presentarán por medio electrónico en la fecha señalada en el cronograma, a los emails pbermudez@cajadelsanta.pe con copia a los emails eperalta@cajadelsanta.pe ; mvalle@cajadelsanta.pe Los archivos de las propuestas deben ir con clave. La clave la enviarán el día 01 de FEBRERO a las 9:00 a.m. a los

email de pbermudez@cajadelsanta.pe y eperalta@cajadelsanta.pe La evaluación la realizarán los funcionarios responsables en acto privado.

Para que una propuesta sea admitida deberá contener los documentos solicitados; así como los términos de referencia indicados
La toma de conocimiento, en cualquier etapa del proceso y hasta antes de la suscripción del contrato, de la existencia de antecedentes negativos evidenciados que pudiera tener el postor y cualquiera de sus representantes o personas vinculadas a aquel, que lo relacione con la investigación o comisión de algún ilícito penal así como la trasgresión de cualquiera de los principios rectores, valores y políticas que regulan la buena marcha institucional, conforme a las normas de prevención vigentes, de tal forma que haga insostenible la relación comercial con la empresa, debido al alto riesgo de pérdida patrimonial o reputacional, será causal de considerar nula la participación del respectivo postor, en forma automática.

INDISPENSABLE:

- Inscribirse como proveedor , llenando las fichas del Anexo N° 01, el cual debe ser remitido al email pbermudez@cajadelsanta.pe el día 27 de enero 2022.

  Para la inclusión en el registro de proveedores de la entidad, las personas naturales y personas jurídicas deben seguir lo estipulado a continuación:

  1.Contar con RUC activo y habido.
  2. No deberá registrar deudas vencidas en el sistema financiero, informadas en central(es) de riesgo con un periodo no menor de tres (03) meses con calificación 100% Normal.
  3. No registrar deuda en cobranza coactiva en SUNAT.
  4. No registrar antecedentes penales ni judiciales (presentar declaraciones juradas) ni estar vinculados a investigaciones o procesos por la comisión de ilícitos penales incompatibles con la naturaleza de la prestación que ofrece el proveedor, a criterio de la entidad. Esta disposición alcanza a las personas naturales y a los representantes de las personas jurídicas que desean incluirse en el registro de proveedores de la entidad.
  5. No estar inhabilitado a contratar con el Estado.
  6. No pertenecer a la lista negativa de acuerdo a los lineamientos de Prevención de lavado de activos y del financiamiento del terrorismo establecidos por la entidad.

CALIDAD:

La calidad debe entenderse como el cumplimiento estricto de las especificaciones técnicas.

CONFORMIDAD DE LA ENTREGA:

La conformidad de las licencias estará a cargo de la oficina directamente comprometida (área usuaria), en un plazo que no excederá de uno (1) a cinco (05) días calendarios de recibido el producto.

FORMA DE PAGO:

Son requisitos de pago los siguientes:

- Que la empresa proveedora haya cumplido con la remisión de la factura correspondiente, según las condiciones establecidas en la Orden de Compra respectiva.

El expediente completo de pago deberá incluir:

- Comprobante de pago.
- Copia de la Orden de Compra debidamente firmado.
- Carta de autorización para el caso de abonos en cuenta.

ANEXO N° 01

DECLARACIÓN JURADA DE DATOS PARA LA INSCRIPCIÓN COMO PROVEEDOR Y/O CONTRAPARTE DE LA CMAC SANTA

Señores
Caja Municipal de Ahorro y Crédito del Santa S.A.
Dpto. de Logística
Chimbote. -

Estimados señores:

El(la) que se suscribe, ……, identificado(a) con DNI Nº ....., en representación de la empresa ……., con RUC N°……; se presenta ante vuestra representada brindando la siguiente información:

DATOS DEL PROVEEDOR Y/O CONTRAPARTE			
Apellidos y Nombres / Razón Social:			
Tipo Documento:		*Nº Documento:*	
Dirección:		*Ciudad:*	
Teléfono(s):		*Años de experiencia:*	
E-mail:		*Página Web:*	
CONTACTO RESPONSABLE			
Apellidos y Nombres:		*Nº DNI:*	
E-mail:		*Nº Celular:*	

IDENTIFICACION DE LOS ACCIONISTAS / SOCIOS / ASOCIADOS		
Apellidos y Nombres	***N° Documento***	***Cargo***

RUBROS EN LOS QUE EL PROVEEDOR Y/O CONTRAPARTE BRINDA SUS PRODUCTOS O SERVICIOS

……, ……. de…… del 20…….

_____

Firma y/o Sello del Proveedor o Contraparte

DECLARACIÓN JURADA DEL PROVEEDOR Y/O CONTRAPARTE

El (la) que suscribe ……..…… identificado con DNI Nº ……..……, representante de la Empresa ……..……..., identificada con RUC Nº……, Declaro Bajo Juramento lo siguiente:

- Cuento con RUC Activo
- No registro deudas vencidas en el sistema financiero, registradas en central(es) de riesgos.
- No registro deuda en cobranza coactiva en SUNAT.
- No Registro antecedentes penales, judiciales, así como no estar inmerso en delito de lavado de activos (Esta disposición alcanza a las personas naturales y a los representantes de las personas jurídicas que desean incluirse en el Registro de Proveedores de la Caja).
- No estar inhabilitado a contratar con el Estado.

……..……, ….... de……..…… del 20……

Firma y/o Sello del Proveedor o Contraparte

ANEXO N° 02

CARTA DE PROPUESTA ECONOMICA
(MODELO)

Señores:
Departamento de Logística.

Proceso Nivel 2 N° 001-2022 CMAC SANTA
"RENOVACION DE LICENCIAMIENTO PARA FIREWALL PERIMETRAL PA-820 POR EL PERIODO DE UN AÑO "

Presente.-

De nuestra consideración,

A continuación, hacemos de conocimiento que nuestra propuesta económica es la siguiente:

Descripción del Producto	PRECIO UNITARIO	PRECIO TOTAL

El monto total de nuestra oferta asciende a……..

El valor de la propuesta incluye todos los tributos, seguros, transportes, inspecciones, costos laborales, conforme a la legislación vigente, así como cualquier otro costo que pueda tener incidencia sobre el costo del bien y/o servicio a contratar.

Chimbote,……

……
Firma, Nombre / Razón social del postor

ANEXO N° 03

DECLARACIÓN JURADA DE OFERTA DE PLAZO DE INSTALACION

Proceso Nivel 2 N° 001-2022 CMAC SANTA
"RENOVACION DE LICENCIAMIENTO PARA FIREWALL PERIMETRAL PA-820 POR EL PERIODO DE UN AÑO"

El que se suscribe, don ……, identificado con DNI Nº..... Representante Legal de....., con RUC. Nº …… **DECLARO BAJO JURAMENTO** que con respecto a los bienes materia del presente proceso de selección que mi oferta es la siguiente:

PLAZO DE INSTALACION (DIAS)	

Lugar, ……

……..……..
Firma y sello del representante legal
Nombre / Razón social del postor