Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

CONTRATO Nº 17/2022

Entre la Facultad Politécnica, domiciliada en Campus de San Lorenzo, República del Paraguay, representada para este acto por la Prof. Ing. Silvia Teresa Leiva León, con Cédula de Identidad N° 1.758.794, denominada en adelante la CONTRATANTE, por una parte, y, por la otra, la empresa NETLOGIC S.R.L con RUC 80015538-6 , domiciliada en Bélgica Nº 210 E/ Guido Spano , de la Ciudad de Asunción, República del Paraguay, representada para este acto por el Sr. Luis Fernando Ismael Teme con C.I 1.033.363, denominada en adelante el PROVEEDOR, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente "CONTRATO DE Adquisición e instalación de router firewall ", el cual estará sujeto a las siguientes cláusulas y condiciones:

1. OBJETO DEL CONTRATO

El objeto del contrato es: Contratación Directa Nº 04/2022 - Adquisición e instalación de router firewall.

2. DOCUMENTOS INTEGRANTES DEL CONTRATO

Los documentos contractuales firmados por las partes y que forman parte integral del Contrato son los siguientes:

1. Contrato;
2. La carta de invitación y sus adendas o modificaciones;
3. Los datos cargados en el SICP;
4. La oferta del proveedor:
5. La resolución de adjudicación del contrato emitida por la contratante y su respectiva notificación.

Los documentos que forman parte del contrato deberán considerarse mutuamente explicativos; en caso de contradicción o discrepancia entre los mismos, la prioridad se dará en el orden enunciado anteriormente

3. DOCUMENTOS ADICIONALES DEL CONTRATO

Los documentos adicionales del contrato son: Las Especificaciones Técnicas y Plan de Entrega. (Anexo I)

4. IDENTIFICACIÓN DEL CRÉDITO PRESUPUESTARIO PARA CUBRIR EL COMPROMISO DERIVADO DEL CONTRATO

El crédito presupuestario para cubrir el compromiso derivado del presente contrato está previsto conforme al Certificado de Disponibilidad Presupuestaria vinculado al Programa Anual de Contrataciones (PAC) con el ID N°: 411.336.

5. PROCEDIMIENTO DE CONTRATACIÓN

El presente Contrato es el resultado del procedimiento de Contratación Directa Nº 04/2022 Adquisición e instalación de router firewall, convocado por la Facultad Politécnica de la UNA. La adjudicación fue realizada según acto administrativo N° 0553/2022.

6. .PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES y/o SERVICIOS.

Ítem	Descripción	Unidad de medida	Presentación	Cantidad	Precio Unitario (IVA Incluido)	Marca	Procedencia	Precio Total (IVA Incluido)
1	Equipo de seguridad de red de firewall (Router Firewall)	Unidad	Unidad	1	156.955.018.-	Fortinet	EE.UU	156.955.018.-
	TOTAL							**156.955.018.-**

El monto total del presente contrato asciende a la suma de: Ciento cincuenta y seis millones novecientos cincuenta y cinco mil dieciocho.

NETLOGIC Legales

El Proveedor se compromete a proveer los Bienes a la Contratante y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.

La Contratante se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en esta carta de invitación.

7. VIGENCIA DEL CONTRATO

La vigencia del presente contrato será: Desde su suscripción hasta el cumplimiento total de las obligaciones.

8. PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE BIENES

Los bienes y/o servicios deberán ser entregados y/o prestados dentro de los plazos establecidos en el Cronograma de Entregas de la Carta de Invitación.

9. ADMINISTRACIÓN DEL CONTRATO

La administración de éste contrato estará a cargo de la División de Control de Contratos.

10. FORMAS Y TÉRMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO

La garantía para el fiel cumplimiento del contrato se regirá por lo establecido en las Condiciones Contractuales de la presente carta de invitación, la cual se presentará a más tardar dentro de los diez (10) días calendarios siguientes a la firma del contrato.

11. CONSTANCIA DE PRESENTACIÓN DE DECLARACIÓN JURADA

El adjudicado deberá en el plazo de quince (15) días calendario desde la firma del presente contrato, presentar ante el administrador de contrato, la constancia o constancias de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, de todos los sujetos obligados en el marco de la Ley N° 6355/19.
En el mismo plazo indicado en el párrafo anterior, se deberá remitir a la convocante la actualización de la mencionada declaración jurada, una vez finalizada la ejecución del presente contrato.

12. MULTAS

Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme con lo establecido en las Condiciones Contractuales de la presente carta de invitación. Llegado al monto equivalente a la Garantía de Fiel Cumplimiento de Contrato, la Contratante podrá aplicar el procedimiento de rescisión de contratos de conformidad al Artículo 59 inc. c) de la Ley N° 2.051/2003 "De Contrataciones Públicas", caso contrario deberá seguir aplicando el monto de las multas que correspondan.
La rescisión del contrato o la aplicación de multas por encima del porcentaje de la Garantía de Cumplimiento del Contrato deberá comunicarse a la DNCP a los fines previstos en el artículo 72 de la Ley N° 2051/2003 "De Contrataciones Públicas", modificado por Ley N° 6716/2021.

13. CAUSALES Y PROCEDIMIENTO PARA SUSPENDER TEMPORALMENTE, DAR POR TERMINADO ANTICIPADAMENTE O RESCINDIR EL CONTRATO.

Las causales y el procedimiento para suspender temporalmente, dar por terminado en forma anticipada o rescindir el contrato, son las establecidas en la Ley N° 2051/2003 y en las condiciones contractuales de la presente carta de invitación.

14. SOLUCIÓN DE CONTROVERSIAS

Cualquier diferencia que surja durante la ejecución del contrato se dirimirá conforme a las reglas establecidas en la legislación aplicable y en las condiciones contractuales.

15. ANULACIÓN DE LA ADJUDICACIÓN

Si la Dirección Nacional de Contrataciones Públicas resolviera anular la adjudicación de la Contratación debido a la procedencia de una protesta o investigación instaurada en contra del procedimiento, y si dicha nulidad afectara al contrato ya suscrito entre LAS PARTES, el Contrato o la parte del mismo que sea afectada por la nulidad, quedará automáticamente sin efecto de pleno derecho, a partir de la comunicación oficial realizada por la DNCP, debiendo asumir LAS PARTES las responsabilidades y obligaciones derivadas de lo ejecutado del contrato.

16. FORMAS Y CONDICIONES DE PAGO

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:
1. Documentos Genéricos:
1. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
2. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
3. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
4. Certificado de Cumplimiento Tributario;
5. Constancia de Cumplimiento con la Seguridad Social;
6. Formulario de Informe de Servicios Personales (FIS)
Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes:
Estará sujeto a la disponibilidad financiera para el ejercicio 2022, una vez que se cumplan los siguientes requisitos
* Emisión del Código de Contratación por parte de la DNCP.
*Emisión de la Orden de servicio y/o compra.
* Nota de conformidad del responsable solicitante del bien adquirido, conforme a las especificaciones técnicas y plan de entrega establecidos.
* Deberá acompañar el cumplimiento a las leyes laborales, previsionales, tributarias o ambientales y los formularios (FIP y FIS Deberá acompañar los formularios (FIP y FIS).

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días posteriores a su presentación.
3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

17. REAJUSTE

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes: El precio adjudicado estará sujeto a reajustes, siempre y cuando el IPC, publicado por el BCP, haya sufrido una variación igual o mayor al quince por ciento (15%) con relación al vigente a la fecha de apertura de ofertas, conforme a la siguiente fórmula: A = P x I.I.B.C.P. A= Precio ajustado de los bienes y/o servicios conexos facturados P= Precio facturado de los bienes y/o servicios conexos ofertados. El reajuste solo será aplicado a solicitud del proveedor, que deberá ser presentado por escrito a la Coordinación de Adquisiciones de Bienes y Servicios de la DNCP, y se dará curso si a convocante cuenta con suficiente disponibilidad presupuestaria, y verifica que se hallan dadas las condiciones para otorgarse el anticipo. La solicitud debe realizarse dentro del mes siguiente al cual se produjeron las variaciones, bajo pena de no poder solicitarlo posteriormente, será aplicado sobre el saldo contractual no ejecutado o sobre los servicios pendientes a ser realizados, posteriores al mes en el cual se produjeron las variaciones . No se reconocerá reajuste de precios si el servicio se encuentra atrasado respecto al plan de entregas aprobado.

Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

En prueba de conformidad se suscriben 3 (tres) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de San Lorenzo, a los 31 días del mes de mayo de 2022.

Firmado por _____ (en nombre del Contratante)
Prof. Ing. Silvia Teresa Leiva León
Decana

Firmado por _____ (en nombre del Contratista)
Sr. Luis Fernando Ismael Teme

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA

ANEXO I

ESPECIFICACIONES TECNICAS

Ítem	Rubro	Código de catálogo	Descripción del bien y/o servicio	Especificaciones Técnicas	Presentación	Unidad de medida
1	543	43222501-001	Equipo de seguridad de red de firewall (Router Firewall)	Características mínimas exigidas **1- Identificación** Cantidad: 1 (uno) Marca - Especificar Modelo - Especificar Numero de Parte - Especificar Procedencia - Especificar Equipo tipo Firewall de Próxima Generación (N€IFW) - Exigido El dispositivo debe estar catalogado corno un appliance de seguridad. Dentro del cuadrante Gartner **2- Dimensión** La solución deberá ser rackeable en racks estándar de 19. 1U como máximo **3- Interfaces** Deberá contar mínimamente con 10 (diez) interfaces GbE RJ45, 4 (cuatro) interfaces SFP (lGbps), 2 (dos) interfaces SFP+ (l0Gbps) y debe tener una interfaz dedicada para administración. Deberá tener la capacidad de ampliación de interfaces a un mínimo de 18 Interfaces adicionales GbE RJ45. De ya contar con la cantidad total de interfaces se considerará este punto como cumplido **4-Almacenamiento** Deberá poseer una capacidad de Almacenamiento de al menos 400 GB en estado sólido. **5-Soporte de Interfaces** Gigabit Ethernet RJ45 y SFP. **6-Administración de la Solución** Interfaz web a través de https, además debe soportar una interfaz CLI mediante conexiones SSH. El sistema operativo de la solución ofertada debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante de la solución.	unidad	unidad

				Deberá permitir la configuración de perfiles de administración, los cuales permitirán la limitación de funciones que pueden ser gerenciados. Deberá soportar SNMP v2 y v3, Syslog remoto La solución deberá soportar un agendado de backup de sus configuraciones y debe poder programarse el envió de dicho backup de manera automática a un repositorio local, FTP o vía email. **7- Autenticación de Usuarios** La solución deberá tener capacidad de integrarse con servidores Radius o LDAP. Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On" El sistema propuesto deberá contar con la funcionalidad de autenticar usuarios de forma transparente con métodos como: Un portal cautivo vía web; a través del uso de un agente instalado en el dispositivo final; obteniendo la información del directorio activo. **8- Alta Disponibilidad de los componentes de la sol** Deberá soportar Alta Disponibilidad sin pérdida de conexiones en caso del fallo de uno los nodos, soporte de Modo Activo- Activo, Activo-Pasivo. Deberá soportar sincronización de sesiones **9- Firewall** Firewall de capa 7 IEEE 802.1Q VLAN, IEEE 802.ad LACP, Deberá permitir la integración con analizadores de tráfico mediante el protocolo sFlow, netflow o IPFix. Ruteo Estático NAT, PAT, NAT con PAT, DHCP Server La solución podrá habilitar políticas de ruteo en IPv6, RIPng, OSPFv2 La solución deberá poder comunicar direccionamiento IPv6 a servicios con IPv4 y viceversa		

NETLOGIC Legales

				BGP v4. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces o VLANs. Deberá ser posible definir políticas de firewall para puertos TCP y UDP independientes en cada interfaz ya sea tráfico entrante o saliente. Las reglas del firewall deberán poder aplicarse a dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios). Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar interfaz física origen, interfaz física destino, direcciones IP origen, dirección IP destino. Deberá soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo y fechas (incluyendo día, mes y año). Capacidad de poder asignar parámetros de traffic shaping o rate liinit diferenciadas para el tráfico en distintos sentidos de una misma sesión. Deberá soportar reglas de firewall en IPv6. Deberá será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces, El dispositivo debe generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS. Capacidad de poder asignar parámetros de traffic shapping o rate limit sobre reglas de firewall en kilobits y Megabits por segundo. **10- Valores de desempeño** Throughput firewall mínimo de 18 Gbps. Throughput NGFW (Control de Aplicaciones + IPS + Web Filter) mínimo de 1,5 Gbps Throughput IPS mínimo de 2,5 Gbps. Throughput de VPN IPSec mínimo de 10 Gbps		

NETLOGIC Legales

				Throughput Threat Protection minimo de 900 Mbps Sesiones Concurrentes (TCP) ininimo de 1.500.000 Nuevas conexiones por segundo minimo de 55.000 **11- Antibornets** Deberá incorporar protección contra Botnets, debe poder bloquear intentos de conexión a servidores de Botnets, debe actualizarse de forma periódica por el fabricante y deberá estar previsto en la oferta la suscripción al servicio durante el periodo de garantía. Deberá soportar conexiones VPN del tipo Site to Slte, client to Site, Soporte de VPNs con algoritmos de cifrado: AES, 3DES, Deberá soportar longitudes de llave para AES de 256 bits, algoritmos de integridad: MD5, SHA-1 y SHA256. La solución deberá contar una aplicación para dispositivos móviles IOS y Android como mínimo, además deberá poder autenticar usuarios de la VPN con Active Directory y Ldap. **12- Ips** Deberá contemplar la suscripción al servicio de actualización de firmas por la duración del periodo de garantía El sistema de prevención de Intrusos deberá estar orientado a la protección de redes y servidores. Deberá soportar la detección de distintos tipos de ataques basándose en firmas actualizables. Deberá poder mitigar los efectos de ataques de denegación de servicios. Deberá contar con mecanismos de detección de ataques basados en reconocimiento de patrones y análisis de protocolos. Deberá poseer mecanismos de protección contra ataques de RPC (Remote Procedure Call). Deberá permitir bloquear tráfico entrante, saliente o ambos correspondientes a determinados países, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.		

NETLOGIC Legales

			El IPS debe poseer configuraciones o firmas predefinidas para servidores que actúen ya sea como webserver, servidor de DNS, servidor de correo o Servidor de Base de Datos Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. Deberá poseer mecanismos de protección contra ataques de Windows o Netbios. Deberá poseer mecanismos de protección contra ataques DNS. El dispositivo debe poder filtrar el tráfico de posibles amenazas con requerimientos inusuales a aplicaciones conocidas o a la arquitectura de red. Deberá proveer información detallada de cada tipo de ataque, Capacidad para manejar perfiles de configuración, Detección de vulnerabilidades, exploits, validación de protocolos, detección de anormalidades, detección de ataques basado en conductas, por ej: múltiples intentos de logueo SSH en pocos segundos, capacidad de crear Excepciones. Deberá contemplar suscripción al servicio de actualizaciones de categorías de filtrado URL que deberá estar vigente durante el periodo de la licencia. Debe poseer la capacidad de filtrar páginas web (URL Filtering). Debe poder aplicar restricción de ancho de banda ya sean para cierto tipo de tráfico, streaming de audio o video, p2p. Capacidad de definir parámetros de Traffic Shaping o rate limit que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo. Capacidad de poder definir prioridad de tráfico, en al menos tres niveles de importancia. Facilidad de incorporar sitios a los cuales naveguen los usuarios, y establecer mediante categorías el acceso de los mismos. Filtrado de contenido basado en		

NETLOGIC Legales

				categorías en tiempo real. Deberá tener la facilidad de crear perfiles para el acceso web, diferenciando el origen ya sean por dirección IP o segmento de red o por usuarios o grupos de usuarios. Los mensajes entregados al usuario por parte del URL FILTER (en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables, facilidad de incorporar sitios a los cuales naveguen los usuarios, y establecer mediante categorías el acceso de los mismos. Deberá contemplar suscripción al servicio de control de aplicaciones que deberá estar vigente durante el periodo de la licencia. Posibilidad de crear políticas granulares para usuarios o grupo de usuarios. Identificar, bloquear o limitar las aplicaciones y las funciones dentro de las aplicaciones. Control Granular de Redes Sociales (Facebook, Twitter, YouTube, Instagram, Goog1e+, LinkedIn, Tagged, Flickr, Pinterest, Badoo, etc.) Por ejemplo si un usuario accede a la red Social Facebook, la herramienta deberá poder permitirle solo acceso de lectura o debe poder deshabilitar las funciones de chat o Posteo de Publicaciones. En el caso de los programas para compartir archivos (peer-to- peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual. Para aplicaciones identificadas deben poder definirse a1 menos las siguientes opciones: permitir, bloquear, registrar en log. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. **13- Identificación y Monitoreo de Usuarios** Deberá poseer capacidades de identificación de usuarios en la red por computadora, por dirección IP, o por grupos. Deberá poder monitorear tráfico tanto de usuarios de un Directorio Activo		

NETLOGIC Legales

como para usuarios Guest.

14- Antivirus

Deberá soportar funcionalidad de Antivirus, Esta funcionalidad deberá estar equipada y activa al momento de la entrega de los equipos. En caso de ser requerido licencias, las mismas deberán ser entregadas con los equipos

15- Reportes

La solución ofertada debe proveer reportes automáticos y personalizables tanto a nivel de estadísticas, indicadores, trafico, consumo, usuarios riesgosos, cumplimiento regulatorio, entre otros integrados en el mismo Firewall sin requerir ninguna plataforma o maquina adicional

La solución deberá poder ofrecer una plataforma adicional opcional de reportes ejecutivos adicionales a la solución de Firewall ofertada y debe ser del mismo fabricante que el firewall

16- Requisitos eléctricos y de funcionamiento

Fuentes de poder interna dual

Voltaje 220V AC, 50/60 Hz.

La solución deberá poseer fuentes internas con cables que se conecten a las PDUs con conectores IEC-60320 C14 que deberán ser provistos por el oferente.

17- Licencia

El licenciamiento de todas las funcionalidades debe
ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

La validez de las licencias debe ser por un periodo de mínimo 60 meses.

18- Capacidad Técnica

El oferente tendrá que contar con al menos 1 técnico de nivel superior según la jerarquía de certificaciones de la marca ofertada. Ej.: CISCO CCNP, FORTINET NSE8, SONICWALL SNSA, ETC

El oferente tendrá que contar con al menos 2 técnicos de nivel medio según la jerarquía de certificaciones de la marca. Ej.: CISCO CCNA, FORTINET NSE4, SONICWALL SNSP, ETC

NETLOGIC Legales

				Los mismos deberán pertenecer al plantel estable de la compañía con una antigüedad no menor a 2 años. Autorización del fabricante El oferente deberá contar con un nivel de partner del tipo Avanzado con el fabricante, entiéndase por ello Elite, Premium, Experto, o similares. Certificados ISO9001, ICSA Labs Cumplimiento CE, FCC, UL, VCCI **19- Capacitación** Se deberá proveer un skill transfer de al menos 8 horas para un máximo de 2 funcionarios de la entidad, y deberá contemplar desde la instalación, configuración y puesta a punto de los componentes de la solución. **20- Instalación** La instalación debe ser del tipo llave en mano. Alcance y Accesorios: El servicio contemplará todos los suministros, actividades de montaje, instalación en general, configuración y puesta en funcionamiento del firewall ofertado. Todos los accesorios necesarios para el buen funcionamiento de los equipos serán proveídos por el oferente. Deberán contemplarse todos los costos necesarios para dar servicio de montaje, instalación y configuración del equipo ofertado. El tiempo máximo para despliegue no deberá superar los 90 días. **21- Soporte** El soporte requerido deberá ser in-situ e incluir la configuración de los equipos en el formato que la convocante lo exija. Se deberá prever un tiempo máximo de respuesta de 4 horas a partir de la comunicación por correo electrónico de la convocante al proveedor. En caso de que el equipo no pueda ser reparado se deberá reemplazar por uno igual o de mayores prestaciones hasta la devolución de equipo reparado; se deberá dejar en funcionamiento todos los servicios con todas las configuraciones. Este soporte es solicitado por el tiempo que dure la Garantía.		

				La empresa oferente deberá contar con un Centro de Atención al Cliente propio de la empresa y que sea con funcionalidad operativa 7x24 (24 horas del día, los 365 días del año), y que cuente con líneas digitales E1 de COPACO para una mayor disponibilidad. Este centro de atención debe tener a disposición técnicos de guardia permanente para los casos de asistencia remota o en situ. Deberá anexar una Declaración Jurada indicando el cumplimiento, así como también la convocante se reserva el derecho de una verificación en sitio del oferente, en caso de que así se requiera. **22- Garantía** Se solicita por 5 (cinco) años. La misma empezara a regir desde la firma del Acta de Recepción Definitiva a ser emitida por la Dirección TIC- FPUNA una vez entregado y configurado en sitio todos los equipos. **23- Catálogos Técnicos** El oferente deberá presentar catálogo de su producto donde indique claramente el cumplimiento de las especificaciones solicitadas. Y todas las documentaciones técnicas adicionales que garanticen el cumplimiento de lo solicitado.		

PLAN DE ENTREGA

Ítem	Descripción del bien y/o servicio	Unidad de medida	Cantidad	Lugar de entrega de los bienes	Fecha final de entrega de los bienes
1	Equipo de seguridad de red de firewall (Router Firewall)	unidad	1	Dirección TIC-FPUNA en coordinación con la División de Patrimonio.	A más tardar dentro de los 60 días hábiles a partir de la recepción del proveedor de la orden de compra.