



# **INVITACIÓN**

## **RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER**

**Gestión 2023**

### **Especificaciones Técnicas**

#### CONFIDENCIALIDAD

La información contenida en este documento es confidencial y propiedad de la empresa YPFB TRANSPORTE S.A. Queda prohibida su copia y/o distribución parcial o total sin el expreso consentimiento del propietario.

## Tabla de contenido

1	INTRODUCCIÓN .....	1
2	ALCANCE DE LA COMPRA .....	1
2.1	CARACTERÍSTICAS TÉCNICAS .....	1
2.1.1	ÍTEM 1: FIREWALLS DE BORDE.....	1
2.1.2	ÍTEM 2: FIREWALL DE DATA CENTER.....	5
2.1.3	ÍTEM 3: PLATAFORMA DE GESTIÓN CENTRALIZADA .....	8
2.1.4	ÍTEM 4: PLATAFORMA DE ANÁLISIS Y REGISTRO DE SEGURIDAD DE RED .....	10
2.1.5	ÍTEM 5: TRANSCEIVERS PARA RED ACI.....	11
3	CAMBIOS Y MODIFICACIONES .....	11
4	SERVICIOS ASOCIADOS .....	12
5	PROVISIÓN.....	15
5.1	PROCEDIMIENTO DE COMUNICACIÓN/ATENCIÓN.....	15
5.2	GARANTÍA Y SOPORTE TÉCNICO .....	15
5.3	INSTALACIÓN.....	15
5.4	PROVISIÓN DE COMPONENTES .....	15
5.5	TRANSFERENCIA DE CONOCIMIENTO.....	16
5.6	ENTRENAMIENTO DE LA SOLUCIÓN OFERTADA POR PARTE DEL FABRICANTE .....	16
6	PRUEBAS DE ACEPTACIÓN.....	16
7	DOCUMENTACIÓN DEL PROYECTO .....	16
7.1	Documentación técnica del proyecto: .....	16
7.2	Acceso a mejores prácticas: .....	17
8	PLAZOS DE ENTREGA.....	17
9	PAGOS.....	18
10	ANEXOS .....	18

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:1
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

## 1 INTRODUCCIÓN

YPFB TRANSPORTE S.A. en cumplimiento a su plan de actualización tecnológica invita a las empresas legalmente establecidas en Bolivia a presentar su propuesta “llave en mano” para la provisión y renovación de equipamiento de seguridad para los Firewalls de Borde y Firewalls de Data center incluyendo las soluciones asociadas para el monitoreo y gestión de los mismos.

## 2 ALCANCE DE LA COMPRA

El alcance de la compra se describe en los siguientes puntos:

### 2.1 CARACTERÍSTICAS TÉCNICAS

#### 2.1.1 ÍTEM 1: FIREWALLS DE BORDE

Se requiere de dos (2) dispositivos de seguridad / Firewall de última generación para renovar la infraestructura de Seguridad Perimetral o de borde actual de YPFB Transporte S.A. A continuación, se detallan las características mínimas que deberá incluir cada equipamiento ofertado, el oferente puede complementar o mejorar su propuesta en función a la validación que le proporcione el fabricante:

Características Generales		
Ítem	Característica	Requerimiento
1.1	Hardware	Equipo de seguridad Firewall de Borde
1.2	Cantidad	2 unidades
1.3	Marca	(Indicar)
1.4	Modelo	(Indicar)
1.5	Arquitectura	Equipo basado en Hardware o appliance del propio fabricante, no debe ser emulado y/o virtualizado).
1.6	Protocolos de Gestión	Puerto de administración remoto. El equipo deberá proveer almacenamiento para registro de fallas, enviar notificaciones y alertas de falla de componentes. Integración al directorio activo, y a sistemas SNMP y registro SYSLOG.
1.7	Ventiladores.	Enfriamiento por aire, utilizando ventiladoras de alto rendimiento en modo redundante.
1.8	Fuentes de energía	Fuente de energía en modo redundante, las cuales deberán permitir el reemplazo en caliente (hot-plug).
1.9	Cables de energía	Cables de energía C13 a C14 estilo PDU
1.10	Administración centralizada	El fabricante de la marca deberá proporcionar una solución apropiada y compatible para la administración centralizada de

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:2
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

		los equipos ofertados, así como almacenamiento de eventos de seguridad. Esta solución deberá de contar con su correspondiente licenciamiento.
1.11	Colecta y retención de logs	El fabricante de la marca deberá proporcionar una solución apropiada y compatible para la colecta y retención de logs que puedan ser generados por el equipamiento ofertado. Esta solución deberá de contar con su correspondiente licenciamiento.
1.12	Garantía y soporte del fabricante.	<p>Garantía integral del equipamiento ofertado por un lapso no menor de cinco (5) años. El fabricante de la marca deberá ofrecer un tiempo de respuesta de tipo 24x7x4, con un tiempo de atención de máximo 4 horas e incluyendo stocks de repuestos en Bolivia.</p> <p>Entiéndase por garantía integral, la garantía que cubre todo el equipo de manera global, así como cada una de las partes que lo componen. Se deberá reemplazar cualquiera de las partes del equipo que presente fallas durante el período de garantía.</p> <p>Contar durante el periodo de garantía, (en caso de fallas en el hardware post venta) con repuestos que garanticen la operación ininterrumpida del equipamiento ofertado, siendo 15 días calendario el plazo máximo para reposición de los accesorios y/o partes dañadas a partir del requerimiento técnico, cada reemplazo, incluirá un informe con los puntos solicitados por YPFB TRANSPORTE S.A.</p> <p>Correr con los costos que se produzcan por la reparación total o parcial del equipamiento, como ser el transporte de su personal técnico, cambio de partes o dispositivos, el transporte de los equipos para su reposición o reparación, etc.</p> <p>Contar con soporte técnico del fabricante para problemas de software y/o configuración, así como contar con actualizaciones de software durante el periodo de garantía.</p>
1.13	Servicios y soporte del fabricante	Servicio de instalación y configuración del equipamiento a cargo de un Especialista de la marca ofertada.
<b>Características / Rendimiento / Capacidades técnicas mínimas solicitadas</b>		
1.14	Certificaciones de seguridad:	ICSALabs: Firewall, IPS, Antivirus, SSL - VPN. NSS Labs: Eficacia de seguridad
1.15	Rendimiento de Firewall:	27 Gbps o superior para paquetes UDP de 1518 bytes; 11 Gbps o superior para paquetes UDP de 64 byte.
1.16	Latencia Firewall paquetes UDP 64 bytes:	Menor a 4,78 µs
1.17	Rendimiento de Firewall en paquetes por segundo:	16,5 Mpps o superior.
1.18	Sesiones concurrentes:	3 millones o superior

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:3
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

1.19	Nuevas sesiones por segundo:	280.000 o superior
1.20	Rendimiento IPS:	5 Gbps o superior
1.21	Rendimiento para NGFW:	3,5 Gbps o superior
1.22	Rendimiento de protección contra amenazas:	3 Gbps o superior
1.23	VPN IPsec Throughput:	13 Gbps o superior
1.24	SSL-VPN throughput:	2 Gbps o superior.
1.25	PKI y certificados:	Mínimamente creación de CSR y soporte SCEP.
1.26	Rendimiento Inspección SSL	4 Gbps
1.27	Control de Aplicaciones:	Detección y control de aplicaciones por diferentes categorías.
1.28	Filtrado Web:	El equipo debe incluir Filtrado Web con modos de inspección basados categorías, en Proxy, en flujo y DNS, detección y bloqueo de URLs maliciosas. En caso de que el Filtrado Web sea definido manualmente debe ser basado en URL, contenido Web y encabezado MIME.
1.29	Inspección SSL	El equipo debe ser capaz de realizar inspección SSL para IPS, control de Aplicaciones, Antivirus, Filtrado Web y DLP.
1.30	Soporte VPN:	<p>El equipo debe tener la posibilidad de ser configurado para soportar redes privadas virtuales redundantes (VPN).</p> <p>El equipo debe permitir múltiples conexiones VPN SSL asociadas a grupos de usuarios.</p> <p>El equipo debe permitir, túneles SSL VPN modo Web, IPsec VPN (con opciones de configuración basados en rutas o en políticas)</p> <p>El equipo debe ser capaz de hacer túneles VPN con equipos de la misma marca o con terceros.</p> <p>El equipo para los túneles VPN debe tener las funciones de Servidor, Cliente y Peer.</p> <p>El equipo debe tener la posibilidad de establecer una VPN sitio a sitio, con una dirección IP dinámica / IP estática.</p>
1.31	Soporte para Clientes VPN	Mínimo de 500 usuarios concurrentes
1.32	Administración remota	Acceso vía navegador HTTPS, SSH, telnet y consola. Soporte de autenticación LDAP, RADIUS y TACACS+.
1.33	Arquitectura de procesamiento independiente:	<p>El equipo debe contar con una arquitectura de procesamiento independiente que incluya mínimamente:</p> <p>Procesadores dedicados a funciones de red como ser aceleración de túneles IP VPN, latencia ultra baja para IPv4/IPv6, fragmentación de paquetes y prevención de</p>

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:4
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

		<p>intrusos basados en anomalías.</p> <p>Procesadores de contenido o coprocesadores dedicados a funciones de seguridad, descifrado de paquetes y procesos de uso intensivo de recursos como detección de patrones para identificación de aplicaciones en tiempo real, correlación de firmas para IPS y procesamiento de antivirus acelerado.</p>
1.34	Instancias Virtuales:	El equipo debe brindar la posibilidad de ser dividido hasta en diez (10) instancias virtuales de dominio que funcionen por separado y puedan ser gestionadas independientemente.
1.35	Puertos de Conexión:	<p>El equipo debe contar mínimamente con 16 puertos GE RJ45.</p> <p>El equipo debe contar mínimamente con 4 x 10 GE SFP+ Slots.</p> <p>El equipo debe contar mínimamente con 8 GE SFP Slots.</p> <p>EL equipo debe contar mínimamente con un puerto USB.</p> <p>El equipo debe contar mínimamente con 1 puertos para administración RJ45 y 1 puerto de HA.</p> <p>El equipo debe contar mínimamente con 1 puerto de consola RJ45.</p>
1.36	Transceiver:	Se deberá incluir un total de dos (2) módulos Transceiver de 10Gb SFP+ de la marca ofertada. <i>(uno por equipo)</i> .
1.37	Alta disponibilidad:	El equipo debe poder funcionar en Alta Disponibilidad en modos: Active/Active, Active/Passive, Clustering.
1.38	Fuente de energía:	El equipo debe tener 2 fuentes de poder (redundantes y Hot Swappable) con capacidad de soportar entrada de energía de 100 -240 V AC, 50 - 60 Hz.
1.39	Servicios y soporte del fabricante:	Servicio de Instalación y configuración del equipamiento a cargo de un Especialista de la marca ofertada.
1.40	Servicios de Migración y optimización de reglas:	Servicio para migración, optimización y configuración de reglas de firewall. <i>(Ver punto 4 Servicios Asociados)</i> .
<b>Licenciamiento y Garantía técnica</b>		
1.41	<p>El equipo ofertado debe incluir licenciamiento de protección de amenazas con mínimamente los siguientes servicios activados:</p> <ul style="list-style-type: none"> <li>- Anti-Malware Protection (AMP)</li> <li>- Antivirus</li> <li>- Botnet</li> <li>- Anti-Spam</li> <li>- Application Control</li> </ul> <p>El licenciamiento debe permitir actualizaciones por el periodo de 5 años.</p>	
1.42	El equipo ofertado debe incluir licenciamiento de Seguridad web para el filtrado de URL y contenido web, video y filtrado de DNS seguro con actualizaciones por el periodo de 5 años.	
1.43	El equipo ofertado debe incluir licenciamiento para el motor de protección IPS con	

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:5
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

	actualizaciones por el periodo de 5 años.
1.44	El equipo ofertado debe incluir Garantía y Soporte de fabricante 24x7 con respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para problemas no críticos. La garantía del fabricante debe contemplar Soporte técnico el reemplazo avanzado de partes RMA con acceso a soporte web y teléfono.
<b>Instalación</b>	
1.45	La oferta debe incluir la instalación y configuración completa de la solución en coordinación con la unidad solicitante. <i>(Ver punto 4 Servicios Asociados).</i>

## 2.1.2 ÍTEM 2: FIREWALL DE DATA CENTER

Se requiere de dos (2) dispositivos de seguridad / Firewall de última generación para renovar la infraestructura de Seguridad de Data Center actual de YPFB Transporte S.A., A continuación, se detalla las características mínimas que deberá incluir cada equipamiento ofertado, el oferente puede complementar o mejorar su propuesta en función a la validación que le proporcione el fabricante.

<b>Características Generales</b>		
<b>Ítem</b>	<b>Característica</b>	<b>Requerimiento</b>
2.1	Hardware	Equipo de seguridad Firewall de Data Center
2.2	Cantidad	2 unidades
2.3	Marca	(Indicar)
2.4	Modelo	(Indicar)
2.5	Arquitectura	Equipo ofertado debe estar basado en Hardware o appliance del propio fabricante, no debe ser emulado y/o virtualizado).
2.6	Protocolos de Gestión	Puerto de administración remoto. El equipo deberá proveer almacenamiento para registro de fallas, enviar notificaciones y alertas de falla de componentes.
2.7	Ventiladores.	Enfriamiento por aire, utilizando ventiladoras de alto rendimiento en modo redundante.
2.8	Fuentes de energía	Fuente de energía redundantes, las cuales deberán permitir el reemplazo en caliente (hot-plug).
2.9	Cables de energía	Cables de energía C13 a C14 estilo PDU
2.10	Administración centralizada	El fabricante de la marca deberá proporcionar una solución apropiada y compatible para la administración centralizada de los equipos ofertados, así como almacenamiento de eventos de seguridad. Esta solución deberá de contar con su correspondiente licenciamiento.
2.11	Colecta y retención de logs	El fabricante de la marca deberá proporcionar una solución

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:6
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

		apropiada y compatible para la colecta y retención de logs que puedan ser generados por el equipamiento ofertado. Esta solución deberá de contar con su correspondiente licenciamiento.
2.12	Garantía y soporte del fabricante.	<p>Garantía integral del equipamiento ofertado por un lapso no menor de cinco (5) años. El fabricante de la marca deberá ofrecer un tiempo de respuesta de tipo 24x7x4, con un tiempo de atención de máximo 4 horas, incluyendo stocks de repuestos en Bolivia.</p> <p>Entiéndase por garantía integral, la garantía que cubre todo el equipo de manera global, así como cada una de las partes que lo componen. Se deberá reemplazar cualquiera de las partes del equipo que presente fallas durante el período de garantía.</p> <p>Contar durante el periodo de garantía, (en caso de fallas en el hardware post venta) con repuestos que garanticen la operación ininterrumpida del equipamiento ofertado, siendo 15 días calendario el plazo máximo para reposición de los accesorios y/o partes dañadas a partir del requerimiento técnico, cada reemplazo, incluirá un informe con los puntos solicitados por YPFB TRANSPORTE S.A.</p> <p>Correr con los costos que se produzcan por la reparación total o parcial del equipamiento, como ser el transporte de su personal técnico, cambio de partes o dispositivos, el transporte de los equipos para su reposición o reparación, etc.</p> <p>Contar con soporte técnico del fabricante para problemas de software y/o configuración, así como contar con actualizaciones de software durante el periodo de garantía.</p>
2.13	Servicios y soporte del fabricante	Servicio de instalación y configuración del equipamiento a cargo de un Especialista de la marca ofertada.
2.14	Integración CISCO ACI	El proponente se deberá especificar las necesidades, tipo de conexión o topología necesaria para su correcta integración con CISCO ACI a nivel de capa 3 (firewall one arm). No se debe modificar la topología actual de la solución ACI.
<b>Características / Rendimiento / Capacidades técnicas mínimas solicitadas</b>		
2.15	Rendimiento de Firewall:	139 Gbps o superior para paquetes UDP de 1518 bytes; 70 Gbps o superior para paquetes UDP de 64 byte.
2.16	Latencia Firewall paquetes UDP 64 bytes:	Menor a 4,12 µs
2.17	Rendimiento de Firewall en paquetes por segundo:	105 Mpps o superior.
2.18	Sesiones concurrentes:	8 millones o superior
2.19	Nuevas sesiones por segundo:	550.000 o superior



	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:7
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

2.20	Rendimiento IPS:	14 Gbps o superior.
2.21	Rendimiento para NGFW:	11,5 Gbps o superior.
2.22	Rendimiento de protección contra amenazas:	10,5 Gbps o superior.
2.23	VPN IPsec Throughput:	55 Gbps o superior
2.24	SSL-VPN throughput:	4.3 Gbps o superior.
2.25	Trabajo basado en políticas:	Usuarios, dispositivos, traffic shapping.
2.26	PKI y certificados:	Mínimamente creación de CSR y soporte SCEP.
2.27	Control de aplicaciones:	Detección y control de aplicaciones por diferentes categorías.
2.28	Inspección SSL:	El equipo debe ser capaz de realizar inspección SSL para IPS, control de Aplicaciones, Antivirus, Filtrado Web y DLP.
2.29	Administración remota:	Acceso vía navegador HTTPS, SSH, telnet y consola. Soporte de autenticación LDAP, RADIUS y TACACS+.
2.30	Virtual domains:	El equipo debe brindar la posibilidad de ser dividido hasta en diez (10) instancias virtuales de dominio que funcionen por separado y puedan ser gestionadas independientemente.
2.31	Arquitectura de procesamiento independiente:	<p>El equipo debe contar con una arquitectura de procesamiento independiente que incluya mínimamente:</p> <p>Procesadores dedicados a funciones de red como ser aceleración de túneles IP VPN, latencia ultra baja para IPv4/IPv6, fragmentación de paquetes y prevención de intrusos basados en anomalías.</p> <p>Procesadores de contenido o coprocesadores dedicados a funciones de seguridad, descifrado de paquetes y procesos de uso intensivo de recursos como detección de patrones para identificación de aplicaciones en tiempo real, correlación de firmas para IPS y procesamiento de antivirus acelerado.</p>
2.32	Puertos de conexión:	<p>El equipo debe contar mínimamente con 16 puertos GE RJ45 Slots.</p> <p>El equipo debe contar mínimamente con 8 GE SFP Slots.</p> <p>El equipo debe contar mínimamente con 4 x 10 GE SFP+ Slots.</p> <p>El equipo debe contar mínimamente con 4 x 25GE SFP28/ 10GE SFP+/ GE SFP Ultra Low Latency Slots.</p> <p>El equipo debe contar mínimamente con 1 puertos para administración RJ45 y 1 puerto de HA.</p> <p>El equipo debe contar mínimamente con 2 puertos USB.</p> <p>El equipo debe contar mínimamente con 1 puerto de consola RJ45.</p>

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:8
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

2.33	Tranceivers:	Se deberá incluir un total de ocho (8) módulos Transceiver de 10Gb SFP+ de la marca ofertada. ( <i>cuatro por equipo</i> ).
2.34	Alta disponibilidad:	El equipo debe poder funcionar en Alta Disponibilidad en modos: Active/Active, Active/Passive, Clustering.
2.35	Trusted Platform Module (TPM)	Mecanismos de seguridad basado en hardware para la protección contra software malicioso y ataques phishing.
2.36	Fuente de energía:	El equipo ofertado debe tener 2 fuentes de poder (redundantes y Hot Plug) con capacidad de auto voltaje 100 -240 V AC, 50 - 60 Hz.
2.37	Servicios y soporte del fabricante	Servicio de Instalación y startup del equipamiento a cargo de un Especialista de la marca ofertada.
2.38	Servicios de Migración y optimización de reglas	Servicio para migración, optimización y configuración de un mínimo de 100 reglas.

#### Licenciamiento y Garantía técnica

2.39	El equipo ofertado debe incluir licenciamiento de protección de amenazas con los siguientes servicios activados: <ul style="list-style-type: none"> <li>- Anti-Malware Protection (AMP)</li> <li>- Antivirus</li> <li>- Botnet</li> <li>- Application Control</li> </ul> El licenciamiento debe permitir actualizaciones por el periodo de 5 años.
2.40	El equipo ofertado debe incluir licenciamiento para el motor de protección IPS con actualizaciones por el periodo de 5 años.
2.41	El equipo ofertado debe incluir Garantía y Soporte de fabricante 24x7 con respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para problemas no críticos. La garantía del fabricante debe contemplar Soporte técnico el reemplazo avanzado de partes RMA con acceso a soporte web y teléfono. por el periodo de 5 años

#### Instalación

2.42	La oferta debe incluir la instalación y configuración completa de la solución en coordinación con la unidad solicitante. ( <i>Ver punto 4 Servicios Asociados</i> ).
------	--

### 2.1.3 ÍTEM 3: PLATAFORMA DE GESTIÓN CENTRALIZADA

Se requiere de una Plataforma de Gestión Centralizada única para administrar los dispositivos de seguridad que forman parte del punto 2.1. A continuación, se detalla las características mínimas que deberá incluir la plataforma ofertada, El oferente puede complementar o mejorar su propuesta en función a la validación que le proporcione el fabricante.

#### Características Generales

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:9
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

Ítem	Característica	Requerimiento
3.1	Software	Plataforma de Gestión Centralizada
3.2	Cantidad	1 unidad
3.3	Modelo	(Indicar)
3.4	Marca	(Indicar)
Características / Capacidades técnicas mínimas solicitadas:		
3.5	Deberá soportar la virtualización a través del hipervisor Vmware vSphere (ESX/ESXi) versión 7.0 o superior.	
3.6	Deberá permitir a los administradores de red, administrar y configurar de forma centralizada las políticas de dispositivos, incluida la actualización de la configuración de red, las reglas de acceso, las definiciones de antivirus, las firmas de prevención de intrusiones, las reglas de acceso y las actualizaciones de software. Deberá permitir la configuración de interfaces de red, rutas, direcciones IPs, redes, tuneles VPN.	
3.7	Deberá permitir la automatización de tareas tales como la copia de seguridad, restauración y actualización de parches.	
3.8	Deberá permitir la integración con soluciones que permitan tener mayor visibilidad con análisis y visualización de datos avanzados para ayudar a los administradores de la plataforma a identificar amenazas y la seguridad de los dispositivos administrados	
3.9	Deberá ofrecer monitoreo en tiempo real de la actividad de los dispositivos de seguridad gestionados, permitiendo la visualización de estadísticas de tráfico, uso de recursos, estado de la interfaz y eventos de seguridad.	
3.10	Deberá permitir la administración de usuarios y control de acceso basado en roles para proteger la plataforma de administración y los datos de configuración.	
3.11	Deberá contar con una interfaz gráfica de usuario (GUI) intuitiva y fácil de usar para facilitar la administración de los dispositivos de seguridad gestionados, además de ofrecer una experiencia de usuario personalizable que se adapte a las necesidades específicas de los administradores.	
3.12	La plataforma deberá soportar Alta disponibilidad (HA).	
Licenciamiento y Garantía técnica		
3.13	Deberá permitir la administración y configuración centralizada de mínimamente 10 dispositivos de seguridad.	
3.14	La plataforma ofertada deberá incluir Garantía y Soporte de fabricante 24x7 con respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para problemas no críticos. por el periodo de 5 años.	
Instalación		
3.15	La oferta debe incluir la instalación y configuración completa de la solución a cargo del especialista de la marca ofertada en coordinación con la unidad solicitante.	
Compatibilidad		

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 0
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

3.16	La plataforma deberá ser de la misma marca de los dispositivos de seguridad propuestos en el punto 2.1 para garantizar al 100% la compatibilidad de las funcionalidades y despliegue. (Manifestar aceptación).
------	--

#### 2.1.4 ÍTEM 4: PLATAFORMA DE ANÁLISIS Y REGISTRO DE SEGURIDAD DE RED

Se requiere de una Plataforma de Análisis y Registro de Seguridad de Red Avanzada. A continuación, se detalla las características mínimas que deberá incluir la plataforma ofertada, El oferente puede complementar o mejorar su propuesta en función a la validación que le proporcione el fabricante

Características Generales		
Ítem	Característica	Requerimiento
4.1	Software	Plataforma de Análisis y Registro de Seguridad de Red Avanzada
4.2	Cantidad	1 unidad
4.3	Modelo	(Indicar)
4.4	Marca	(Indicar)
Características / Capacidades técnicas mínimas solicitadas:		
4.5	Deberá soportar la virtualización a través del hipervisor Vmware vSphere (ESX/ESXi) 7.0 o superior.	
4.6	Deberá permitir el registro y análisis de eventos de seguridad de forma centralizada para el análisis de los mismos sobre los dispositivos de seguridad administrados.	
4.7	Deberá permitir un análisis avanzado de seguridad que permita detectar patrones y tendencias en los registros de eventos de seguridad.	
4.8	Deberá permitir el análisis de tráfico, análisis de amenazas, análisis de comportamiento y análisis de vulnerabilidades.	
4.9	Deberá permitir a los administradores de la plataforma crear informes personalizados sobre los registros de eventos de seguridad.	
4.10	Deberá permitir la administración de usuarios y control de acceso basado en roles para proteger la plataforma de administración y los datos de configuración.	
4.11	Deberá contar con una interfaz gráfica de usuario (GUI) intuitiva y fácil de usar.	
Licenciamiento y Garantía técnica		
4.12	La plataforma deberá permitir una cuota diaria mínima de 5GB/día para el registro de logs y analísticas.	
4.13	La plataforma ofertada deberá incluir una suscripción de IOC (indicadores de compromiso) para detectar hosts de usuarios comprometidos, con actualizaciones por el periodo de 5 años o superior.	

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 1
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

4.14	La plataforma ofertada deberá incluir una suscripción de servicio de automatización de seguridad y el servicio de detección de brotes por el periodo de 5 años.
4.15	La plataforma ofertada deberá incluir Garantía y Soporte de fabricante 24x7 con respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para problemas no críticos. por el periodo de 5 años.
<b>Instalación</b>	
4.16	La oferta debe incluir la instalación y configuración completa de la solución a cargo del especialista de la marca ofertada en coordinación con la unidad solicitante.
<b>Compatibilidad</b>	
4.17	La plataforma deberá ser de la misma marca de los dispositivos de seguridad propuestos en el punto 2.1 para garantizar al 100% la compatibilidad de las funcionalidades y despliegue. (Manifestar aceptación)

#### 2.1.5 ÍTEM 5: TRANSCEIVERS PARA RED ACI

Se requieren Transceivers adicionales para conectar los equipos de seguridad a la red ACI de la marca CISCO.

Características Generales		
Ítem	Característica	Requerimiento
5.1	Hardware	Transceivers Cisco 10 Gbps.
5.2	Cantidad	10 unidades
5.3	Modelo	SFP-10G-SR
5.4	Marca	CISCO

### 3 CAMBIOS Y MODIFICACIONES

Las modificaciones para reemplazo o mejoras a cualquier punto de este pliego, deberán ser consultadas y aprobadas por el equipo evaluador de YPFB TRANSPORTE S.A. durante el tiempo establecido para consultas y recepción de propuestas, para ello el ofertante deberá utilizar el siguiente

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas: 1 2
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

formato:

Ítem	Numero de parte a reemplazar	Numero de parte Propuesto	Descripción del Componente propuesto	Motivo del Cambio

Se aclara que cualquier modificación que no esté consensuada con YPFB TRANSPORTE S.A., será considerada como incumplimiento y descalificación.

#### 4 SERVICIOS ASOCIADOS

4.1. La compra de los componentes, software de administración, equipos, licencias y soluciones listadas anteriormente será bajo la modalidad "llave en mano" AUTOSUFICIENTE, donde por solución autosuficiente se entiende:

- Todos los elementos de hardware, software, licencias, materiales y servicios, que no hayan sido contemplados por el proveedor luego de la revisión de especificaciones y consultas durante la licitación, serán enteramente responsabilidad del oferente, sin costo alguno para YPFB TRANSPORTE S.A.

4.2. Las configuraciones y especificaciones descritas en el punto "2 - ALCANCE DE LA COMPRA", contemplan únicamente los principales componentes, es responsabilidad del proveedor la validación e inclusión de otros componentes internos y/o externos que sean requeridos para el correcto funcionamiento de los equipos, como ser: ventiladores internos, cables de conexión interna, adaptadores, cables, terminales de energía eléctrica, kits para montaje y cualquier otro material necesario para el correcto funcionamiento de los equipos.

4.3. La entrega del equipamiento y accesorios deberá incluir soporte tanto de hardware, software y servicios de manera directa del fabricante hacia YPFB TRANSPORTE S.A., lo cual se aplicará de acuerdo a lo especificado en cada equipo.

4.4. Se deberá incluir un servicio de instalación y configuración, de acuerdo a los siguientes requerimientos, pero no limitado a:

#### Firewall de Borde:

- La instalación, montaje y configuración de todo el equipamiento, incluyendo los servicios asociados que deberá contemplar todas las configuraciones necesarias, para el correcto funcionamiento del equipamiento ofertado.
- La implementación y puesta en marcha del equipamiento ofertado, deberá ser realizado por ingenieros certificados en la marca.
- Es importante mencionar que durante la implementación de este equipamiento; se deberán

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas: 1 3
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

tomar todas las previsiones necesarias para evitar la caída de servicios asociados a la conexión LAN de los servidores hacia el segmento de usuarios de YPFB TRANSPORTE S.A.

- Instalación y configuración del firewall en alta disponibilidad en modo activo/pasivo.
- Migración, optimización y configuración de reglas de firewall en producción en la red de borde de YPFB Transporte al nuevo firewall ofertado; 350 reglas de firewall aproximadamente. Estas reglas estarán orientadas a la protección de los principales servidores y servicios que brinda la Dirección de Tecnologías de la Información dentro de YPFB TRANSPORTE S.A.
- Configuración de perfiles de seguridad IPS/Antivirus y otros según lo aconseje las buenas prácticas de seguridad para cada regla de Firewall.
- Configuración de NATs para publicación de servicios y salida a Internet.
- Configuración de balanceo de tráfico para la salida a Internet.
- Configuración de protocolo de enrutamiento dinámico OSPF con redistribución de rutas estáticas.
- Configuración de VPN Corporativa SSL en alta disponibilidad, integrada con servidor Radius Cisco ISE.
- Configuración de protocolo WCCP para redirección de tráfico proxy.
- Configuración de TACACS+ e integración con servidor Cisco ISE.
- Integración con sistema propio u otro para la capacidad de crear reglas de Firewall basado en identidades como ser nombre de usuarios.
- Integración a la plataforma de gestión centralizado y plataforma de análisis y registro de seguridad de red ofertado.
- Integración con servidor SYSLOG centralizado QRADAR
- Configuración de protocolo SNMP para monitoreo.

### **Firewall de Data center:**

- La instalación, montaje y configuración de todo el equipamiento, incluyendo los servicios asociados que deberá contemplar todas las configuraciones necesarias, para el correcto funcionamiento del equipamiento ofertado.
- La implementación y puesta en marcha del equipamiento ofertado, deberá ser realizado por ingenieros certificados en la marca.
- Es importante mencionar que durante la implementación de este equipamiento; se deberán tomar todas las previsiones necesarias para evitar la caída de servicios asociados a la conexión LAN de los servidores hacia el segmento de usuarios de YPFB TRANSPORTE S.A.



	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 4
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

- Servicio de instalación y configuración de un clúster en alta disponibilidad bajo las siguientes modalidades: Active/Active, Active/Passive. Esta configuración deberá ser validada y acordada entre el área de Redes y telecomunicaciones de YPFB TRANSPORTE S.A. y la empresa a cargo de la implementación de la solución.
- Creación y configuración de 2 (dos) dominios virtuales o instancias destinadas a gestionar y controlar por separado el tráfico proveniente de las redes de servicios de TI/Corporativo y SCADA. El dominio virtual asignado a SCADA deberá contar con su correspondiente licenciamiento para inspección de protocolos OT en base a firmas industriales.
- Conexión e integración en capa 3 del nuevo Firewall con la red de data center ACI (firewall one arm). No se debe modificar la topología actual de la solución ACI.
- Servicio de migración, optimización y configuración de 100 reglas para los nuevos firewall's de data center. Estas reglas estarán orientadas a la protección de los principales servidores y servicios que brinda la Dirección de Tecnologías de la Información dentro de YPFB TRANSPORTE S.A.
- La empresa a cargo de la implementación de la solución, deberá contemplar una solución para la colecta y retención de logs que puedan generar los equipos ofertados, YPFB TRANSPORTE S.A. proporcionará el volumen donde se almacenaran estos logs.
- Configuración de perfiles de seguridad IPS/Antivirus y otros según lo aconseje las buenas prácticas de seguridad para cada regla de Firewall.
- Configuración de protocolo de enrutamiento dinámico OSPF o enrutamiento estático.
- Configuración de TACACS+ e integración con servidor Cisco ISE.
- Integración con sistema propio u otro para la capacidad de crear reglas de Firewall basado en identidades como ser nombre de usuarios.
- Integración a la plataforma de gestión centralizado y plataforma de análisis y registro de seguridad de red ofertado.
- Integración con servidor SYSLOG QRADAR centralizado.
- Configuración de protocolo SNMP para monitoreo.

4.5. Toda la configuración de los dispositivos de seguridad se debe realizar en coordinación con la Jefatura de Redes y Soporte Técnico. Se proporcionará información basada en los estándares de configuración y arquitecturas de red de YPFB Transporte S.A.

4.6. La ubicación del servicio deberá ser ejecutada en la Oficina Central de YPFB Transporte S.A. ubicada en la avenida Doble Vía la Guardia Km 7 ½.

4.7. De presentarse la necesidad de recurrir al servicio de RMA del fabricante y la reposición de partes, el proveedor deberá gestionar el caso para el reemplazo de partes en coordinación con el fabricante y el Jefe de Redes y Soporte Técnico de YPFB TRANSPORTE S.A.. Se



	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:1 5
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

debe garantizar la provisión sin cargo adicional de partes y materiales requeridos para reemplazar las partes defectuosas del hardware bajo soporte.

## 5 PROVISIÓN

A continuación, se especifican las condiciones requeridas

### 5.1 PROCEDIMIENTO DE COMUNICACIÓN/ATENCIÓN

En el marco del desarrollo de este proyecto, la empresa oferente deberá designar un encargado de proyecto que trabajará bajo la supervisión del encargado del proyecto o Jefe de Redes y Soporte Técnico de YPFB TRANSPORTE S.A., en el marco del desarrollo de este proyecto o para aplicación del soporte de garantía cuando sea solicitado.

### 5.2 GARANTÍA Y SOPORTE TÉCNICO

Toda la solución ofertada para los equipos y software deben contar con garantía del fabricante por el periodo de cinco (5) años con un nivel de SLA 24x7 como se lo especifica en las tablas de configuración de cada ítem en el punto 2.1.

Las garantías, licenciamiento y/o contratos de soporte deberán ser registrados y/o vinculados al encargado de proyecto de YPFB TRANSPORTE S.A.

Los equipos ofertados, deberán ser originales, nuevos de fábrica, los mismos deben encontrarse disponibles para su venta sin que estos figuren con fecha de fin de orden ni fecha de fin de soporte. El proveedor deberá presentar una documentación emitida por el fabricante que demuestre lo solicitado.

El proveedor, como parte de la garantía del fabricante de los equipos deberá procesar de ser necesario el RMA del equipamiento que cuente con soporte, de manera local, recibiendo y entregando los equipos en oficinas de YPFB TRANSPORTE S.A. sin que esto represente un costo adicional.

El personal asignado para la ejecución de este proyecto deberá acreditar su idoneidad para el trabajo por medio de certificados (*ver punto 10 Anexos*).

### 5.3 INSTALACIÓN

El proveedor deberá presentar como parte de su propuesta un cronograma de trabajo (Diagrama de Gantt) detallando todas las tareas que serán realizadas, los recursos asignados a las mismas y la relación entre las diferentes tareas, de forma tal que se pueda hacer un adecuado seguimiento de la implementación conociendo la ruta crítica del proyecto.

### 5.4 PROVISIÓN DE COMPONENTES

Todos los componentes listados en la tabla de especificaciones dentro del punto “2. Alcance de la compra” y aquellos que estén en el punto “4. Servicios asociados” así como otros que no formen parte del equipamiento o solución, deberán ser incluidos en la cotización y podrán ser entregados como elementos independientes en sus respectivas cajas o contenedores.

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 6
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

El licenciamiento y otros intangibles que formen parte de la solución, de ser requerido por el encargado de proyecto de YPFB TRANSPORTE S.A., deben ser entregados en cuanto el fabricante procese la activación de los mismos.

## 5.5 TRANSFERENCIA DE CONOCIMIENTO

La transferencia de conocimiento de la solución instalada, consistirá de un taller en el cual se detallen todas las actividades que se realizaron para la implementación del presente proyecto, tanto a nivel de hardware y software.

La transferencia de conocimiento deberá ser bajo la modalidad presencial o virtual de por lo menos cuatro (4) horas para el personal designado por YPFB TRANSPORTE S.A.

Las fechas y horarios del taller serán definidas previa coordinación con el encargado del proyecto por parte de YPFB TRANSPORTE S.A.

## 5.6 ENTRENAMIENTO DE LA SOLUCIÓN OFERTADA POR PARTE DEL FABRICANTE

El entrenamiento de la solución ofertada, consistirá de un curso oficial proporcionado por el fabricante de la solución.

La transferencia de conocimiento deberá ser bajo la modalidad virtual, para cuatro (4) personas designadas por YPFB TRANSPORTE S.A.

Las fechas y horarios del entrenamiento serán definidas previa coordinación con el encargado del proyecto por parte de YPFB TRANSPORTE S.A.

## 6 PRUEBAS DE ACEPTACIÓN

El proponente deberá entregar un listado de las pruebas de aceptación a realizar. Estas pruebas servirán para garantizar la correcta instalación, configuración y alta disponibilidad de la solución y deberán incluir mínimamente los detalles más relevantes de relacionados con la migración de reglas de firewall.

## 7 DOCUMENTACIÓN DEL PROYECTO

El proponente deberá adjuntar documentación técnica para respaldar su oferta, la cual debe provenir de catálogos del fabricante que formarán parte de la propuesta. Así mismo el proponente debe indicar el sitio WEB (URL) donde obtener información técnica para sustentar la documentación entregada.

### 7.1 Documentación técnica del proyecto:

La empresa proveedora deberá entregar toda la documentación técnica, Informe "As-Built", manuales de Instalación y configuración, referencia de comandos, configuración de los equipos, operación, administración y mantenimiento, topología física y lógica en formato Impreso y digital una vez concluida la Implementación. También se debe contemplar:

	<b>ESPECIFICACIONES TÉCNICAS</b>	
	PROYECTO: Telecomunicaciones / Centro de Computo	Hojas:1 7
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER	

- Detalle del equipamiento entregado con cantidad y números de serie. (Tabla con números de serie).
- Diagrama de los equipos a ser entregados (Front/Back).
- Diagrama de conexión de redes LAN del equipamiento entregado.
- Listado de licencias o suscripciones que deben estar asociadas a una cuenta de administración de YPFB TRANSPORTE S.A.

Tabla de configuración de las redes LAN con la siguiente información mínima:

- Equipo.
- Red.
- VLAN.
- Puerto de tarjeta.
- Tipo Puerto.

Todo equipamiento y conexión debe incluir el etiquetado de los cables acorde al estándar definido por YPFB TRANSPORTE S.A.

Toda la documentación técnica deberá ser entregada en un folder, impreso a colores, así también en su versión digital y en formatos editables.

Todos los documentos deben tener un histórico de revisión.

## 7.2 Acceso a mejores prácticas:

La empresa proveedora durante la implementación deberá otorgar y compartir soluciones basadas en las mejores prácticas para conseguir la consistencia y el soporte adecuado, contando además con la posibilidad de acceder a la infraestructura y base de conocimientos mundiales de fábrica, vía Internet. especificar URL de soporte, foros y otros del fabricante y credenciales de ingreso (ID) si se requiriese.

## 8 PLAZOS DE ENTREGA

Se deberán considerar los siguientes plazos de entrega:

- Entrega de todos los equipos en almacén YPFB TRANSPORTE S.A.: hasta 90 días calendario luego de recibida la orden de compra.

Se deberán considerar los siguientes plazos de instalación de equipos:

- Puesta en operación y pruebas: hasta 20 días calendario luego de la recepción de los equipos.
- En caso de encontrarse algún problema durante las pruebas de aceptación, el proveedor tendrá un plazo de 10 días luego de reportada la falla para resolverlo.

El tiempo total de entrega previsto para este proyecto será de 120 días calendario.

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 8
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

## 9 PAGOS

El pago se realizará:

- 100% al término satisfactorio de la entrega de la solución, montaje, instalación del equipamiento hardware adquirido, transferencia de conocimiento y entrega de la documentación del proyecto.

## 10 ANEXOS

A continuación, se detalla la información que deberá ser entregada con la propuesta técnica, la misma deberá estar correctamente ordenada y enumerada según el siguiente listado. Se deja en claro que la ausencia de esta información en la propuesta entregada, la no entrega en el tiempo establecido, y/o el no cumplimiento de alguno de los puntos mencionados será causal de descalificación directa.

- 1) La empresa ofertante deberá presentar certificados del fabricante donde demuestre y avale:
  - a. La garantía y condición de los equipos, avalando que estos son nuevos y de fábrica.
  - b. Condición de canal autorizado por el fabricante para el territorio de Bolivia.
  - c. Certificados de especialización.
- 2) La empresa ofertante deberá tener una antigüedad en el rubro tecnológico mínimamente de cinco (5) años comercializando en el territorio de Bolivia. Deberá presentar su matrícula de comercio adjunto.
- 3) La empresa ofertante deberá cumplir con los siguientes requisitos:
  - a) Contar con al menos dos (2) personas en Bolivia que posean certificación técnica vigente a nivel "Profesional en seguridad", esta certificación deberá ser propio del fabricante del equipamiento ofertado, se aclara que no se tomará en consideración las certificaciones de ventas o 'pre-sales'. Se deberá proporcionar enlaces (links) de referencia donde se pueda constatar la veracidad y vigencia de la certificación presentada.
  - b) Contar con al menos una (1) persona con certificación técnica vigente a nivel de CCNP Enterprise y/o CCNP Security para apoyar en la configuración e integración del Firewall de Data Center a la red Cisco ACI perteneciente a YPFB Transporte S.A.
- 4) En referencia al punto anterior. El ofertante deberá presentar:
  - a) Curriculum Vitae del personal que realizará la implementación donde se demuestre la experiencia e idoneidad requerida en los ítems que instalará.
  - b) Organigrama y cargo dentro del marco de ejecución del proyecto.
  - c) Deberá ser personal de planta que tenga una antigüedad de por lo menos 6 meses en la empresa a cargo del proyecto (presentar documentos de respaldo como ser seguro de salud CNS o AFP).

	<b>ESPECIFICACIONES TÉCNICAS</b>		Hojas:1 9
	PROYECTO: Telecomunicaciones / Centro de Computo		
	TITULO: RENOVACIÓN DE FIREWALLS DE BORDE Y DE DATA CENTER		

- 5) Detalle de trabajos similares efectuados anteriormente:
  - a) Se deberá referenciar al menos una (1) empresa en Bolivia (nombre, cargo, teléfono y/o correo electrónico) donde haya instalado los ítems ofertados o similares (solo hardware).
  - b) Antigüedad de la instalación (cuándo se realizó).
- 6) Documentación técnica de los equipos y/o software ofertado.
- 7) Nombre y teléfono de contacto de la persona a cargo del proyecto como interlocutor válido para YPFB TR para todos los requerimientos comerciales y técnicos, esta persona deberá tener un celular con disponibilidad 24x7 (horas x días a la semana). Esta persona será también el encargado de atender cualquier reclamo asociado a la provisión de equipos y/o los servicios asociados hasta la finalización del proyecto.