P.E.T

PLIEGO DE ESPECIFICACIONES TÉCNICAS

"PROVISIÓN DE SOPORTE PARA FIREWALL DE NUEVA GENERACION Y SISTEMA DE GESTION DE EVENTOS DE SEGURIDAD"

ÍNDICE DE CONTENIDOS

ARTÍCULO 1°. INTRODUCCIÓN 3
DENOMINACIONES ***3***
ARTÍCULO 2°. ALCANCE 4
Ítem A: NGFW FORTIGATE - Suscripción con el fabricante de la solución - Fortinet (software e infraestructura relacionada). ***4***
Ítem B: SIEM FORTISIEM - Suscripción con el fabricante de la solución - Fortinet (software). ***5***
ARTÍCULO 3°. CONSIDERACIONES GENERALES. 6
3.1 REQUISITOS TÉCNICOS ***6***
3.2 PLAZO DE EJECUCIÓN ***6***
3.3 CONDICIONES DE ENTREGA Y SOPORTE ***6***
3.4. CAPACIDADES Y ANTECEDENTES DEL OFERENTE ***6***
3.5 ESPECIFICACIONES PARA LA PRESENTACIÓN DE LAS PROPUESTAS TÉCNICAS ***7***
3.6 ESPECIFICACIONES PARA LA PRESENTACIÓN DE PROPUESTAS ECONÓMICAS ***8***
3.7. CONSIDERACIONES DE SEGURIDAD INFORMÁTICA ***8***
3.8. CERTIFICACIÓN ***9***
3.9. ADJUDICACIÓN ***9***
ANEXO A – PLANILLA DE COTIZACIÓN ***10***

ARTÍCULO 1°. INTRODUCCIÓN

El presente Pliego tiene por objeto establecer las Especificaciones Técnicas a las que se ajustará la contratación y todo el procedimiento asociado directa o indirectamente con la **PROVISIÓN DE SOPORTE PARA FIREWALL DE NUEVA GENERACION Y SISTEMA DE GESTION DE EVENTOS DE SEGURIDAD.**

Los equipos y software mencionados en el presente pliego se encuentran alojados en las instalaciones de ARSAT en Benavidez

DENOMINACIONES

A los fines de su empleo en las cláusulas establecidas en el presente pliego y demás documentos relativos a este PET, se utilizan las siguientes denominaciones:

ARSAT: Empresa Argentina de Soluciones Satelitales SA, brinda recursos de computación, administrados por la Secretaría de Innovación Pública.

FIREWALL: Dispositivo de seguridad de red que monitorea y controla el tráfico de red entrante y saliente según reglas de seguridad predefinidas. Su función principal es bloquear o permitir el paso de datos de acuerdo con criterios específicos para proteger los sistemas informáticos de accesos no autorizados y amenazas externas.

FIREWALL DE NUEVA GENERACIÓN (NGFW): Tipo de firewall avanzado que incluye características de filtrado de paquetes, inspección de tráfico en profundidad y protección contra amenazas más sofisticadas que los firewalls tradicionales.

FORTISIEM: Sistema de Gestión de Información y Eventos de Seguridad de la marca FORTINET que proporciona monitoreo y análisis de los eventos de seguridad de la red, ayudando en la detección y respuesta ante incidentes.

FORTIGATE: Firewall de nueva generación (FNGW) de la marca FORTINET.

FORTIGUARD: Plataforma de seguridad proporcionada por FORTINET que ofrece servicios de protección avanzados casi en tiempo real, como protección contra virus, filtrado web, prevención de intrusiones, etc.

FORTINET: Proveedor especializado en ciberseguridad, ofreciendo soluciones como firewalls, SIEM y otras herramientas para proteger redes e infraestructura tecnológica.

HERRAMIENTA: Para referirse a la parte del SOFTWARE comercialmente desarrollado por el fabricante del mismo, no destinado particularmente a SOFSA, sobre el que se otorgan derechos de uso no exclusivo, que permite implementar la solución sin las modificaciones específicas para SOFSA.

LICENCIAS DE SOFWARE: Contrato con el fabricante de un software que permite a SOFSA utilizar un producto bajo ciertas condiciones, especificando el período de validez y las restricciones de uso.

MEJORES PRÁCTICAS: Para referirse a las estrategias, actividades o enfoques que a través de la investigación y/o experiencia han demostrado ser efectivas, ya sea en relación con la ejecución de los procesos y su implementación a través de la utilización del SOFTWARE y/o en el desarrollo de las actividades de negocio.

PET: Para referirse al presente Pliego de Especificaciones Técnicas.

PROYECTO: Para referirse al conjunto de documentos, requisitos, propuestas, planes, talleres de trabajo, especificaciones y toda información que defina el SOFTWARE y los SERVICIOS ofrecidos por el OFERENTE.

SERVICIO: Para referirse a las tareas que realiza personal técnico especializado certificado en las tecnologías sobre las que realiza los trabajos.

ARTÍCULO 2°. ALCANCE

El presente pliego tiene por objetivo especificar las cuestiones técnicas referidas a la provisión de servicios de soporte estándar con el fabricante FORTINET de las soluciones FORTIGATE y FORTISIEM para los productos indicados en los siguientes ítems:

Ítem A: NGFW FORTIGATE - Suscripción con el fabricante de la solución - Fortinet (software e infraestructura relacionada).

Se requiere la suscripción con el fabricante de la solución de Fortinet para los productos y licencias indicados en el siguiente cuadro:

Tipo	Producto	Número de serie
Firewall de Red	FORTIGATE 1800F	FG180FTK22901977
Firewall de Red	FORTIGATE 1800F	FG180FTK22902064
Licencia - FortiAnalyzerVM	FortiAnalyzer VM upgrade license for 25 GB/Day and 10 TB storage capacity	FAZ-VMTM23007401
Licencia - FortiToken Mobile	100 FortiTokenMobile software license key	
Suscripción	Subscription license for the FortiGuard Indicator of Compromise (IOC) (1-26 GB)	

Tipo	Producto	Número de serie
Suscripción	FortiGuard Outbreak Alert Service (1-26 GB)	
Suscripción	Premium Web Support (1-26 GB)	
Suscripción	Premium Comprehensive Support (1-26 GB)	
Suscripción	OS Updates (1-26 GB)	

La suscripción con el fabricante debe incluir como mínimo la posibilidad de descargar las actualizaciones de software, el escalamiento de incidentes que no puedan ser resueltos de forma local (Fortinet actúa como soporte de tercer nivel) y un servicio de RMA, en caso de una falla de hardware.

Ítem B: SIEM FORTISIEM - Suscripción con el fabricante de la solución - Fortinet (software).

Se requiere la suscripción con el fabricante de la solución de Fortinet para los productos y licencias indicados en el siguiente cuadro:

Tipo	Producto	Número de serie
SIEM	FORTISIEM ve para 175 dispositivos	FSMP000000014516
Licencia - AIO Device	Base perpetual license for Security and Monitoring Services. Manages 50 devices and 500 EPS	
Licencia - AIO Device	Add 25 devices and 250 EPS for perpetrual license	
Licencia - AIO Device	Add 100 devices and 1000 EPS for perpetrual license	
Suscripción	Premium Web Support (for 1 - 300 points) for FortiSIEM Software deployments	
Suscripción	Premium Comprehensive Support (for 1 - 300 points) for FortiSIEM Software deployments	
Suscripción	Updates (for 1 - 300 points) for FortiSIEM Software deployments.	

La suscripción con el fabricante debe incluir como mínimo la posibilidad de descargar las actualizaciones de software, el escalamiento de incidentes que no puedan ser resueltos de forma local (Fortinet actúa como soporte de tercer nivel) y un servicio de RMA, en caso de una falla de hardware. Asimismo, la suscripción habilita la colección de eventos necesarios para analizar el tráfico de los servidores incluidos en la infraestructura de SOFSA.

ARTÍCULO 3°. CONSIDERACIONES GENERALES.

3.1 REQUISITOS TÉCNICOS

El proveedor deberá garantizar que:

- Las licencias y servicios sean originales y provistos directamente por FORTINET o un distribuidor autorizado.
- Se garantice la compatibilidad con la infraestructura actual.
- Se mantenga la continuidad del servicio sin interrupciones.
- Se brinde soporte técnico especializado en caso de incidencias.

3.2 PLAZO DE EJECUCIÓN

- El plazo de las licencias del Renglón 1 será por 17 meses a partir de la suscripción del Acta de Inicio.
- El plazo de las licencias del Renglón 2 será por 19 meses a partir de la suscripción del Acta de Inicio

3.3 CONDICIONES DE ENTREGA Y SOPORTE

- La entrega de las licencias debe realizarse en formato digital con los códigos de activación correspondientes.
- Se debe incluir documentación técnica y manuales de instalación/configuración.
- Se debe ofrecer soporte técnico de cada proveedor durante el periodo de vigencia de la licencia.

3.4. CAPACIDADES Y ANTECEDENTES DEL OFERENTE

El OFERENTE deberá:

- Contar con una organización con las capacidades y los antecedentes requeridos.
- Presentar experiencia de trabajos similares comprobable en organismos de similar naturaleza, complejidad y volumen a la descripta en el presente pliego, ejecutadas y en ejecución, en los últimos cinco (5) años, donde conste nombre de la contratación, comitente, características técnicas mencionando principales tareas, plazo de ejecución, lugar de ejecución, fecha de comienzo y de recepción provisoria y/o definitiva.
- Disponer de recursos humanos en cantidad y calidad suficientes para sostener en el tiempo el nivel de servicio del soporte solicitado.

- Disponer de salud económica financiera que asegure la continuidad del servicio de soporte (2 últimos balances con utilidad).

Es MANDATORIO que el referente técnico del OFERENTE posea experiencia en las soluciones requeridas y resida en Argentina para participar de actividades en sitio presencial, en caso de ser requerido por Trenes Argentinos.

Con el fin de reducir riesgos, mejorar la transparencia y responsabilidad, cumplir con las leyes y regulaciones, será altamente valorado que el OFERENTE posea o se encuentre en proceso de certificación de las siguientes ISO:

- ISO 14001 GESTION y EVALUACION AMBIENTAL
- ISO 37001 SISTEMA DE GESTION ANTISOBORNO
- ISO 27001 SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
- ISO 9001 SISTEMA DE GESTIÓN DE CALIDAD SOBRE EL SERVICIO DE SOPORTE

El personal del OFERENTE deberá trabajar en conjunto con el personal técnico designado por SOFSA, de acuerdo a las especificaciones establecidas en el presente pliego.

3.5 ESPECIFICACIONES PARA LA PRESENTACIÓN DE LAS PROPUESTAS TÉCNICAS

A continuación, se detalla la documentación a presentar por el OFERENTE:

- Propuesta de servicios: Descripción de la propuesta de servicios, niveles de escalamiento, contactos y niveles de servicio.

Si el oferente es un canal de venta de la marca propuesta, deberá acreditar documentación de forma fehaciente

- Carta emitida por la marca representada, declarando que es canal certificado y autorizado para cotizar en la presente licitación.

El OFERENTE deberá presentar una propuesta válida para la totalidad de los ítems de la contratación.

Todo documento que el OFERENTE considere que deba ser firmado por SOFSA luego de la adjudicación (por ej. Contrato de confidencialidad, de propiedad intelectual, etc.), deberá ser presentado conjuntamente con la oferta técnica. En tal sentido, se advierte que los citados documentos serán suscriptos con carácter exclusivo entre SOFSA y quien resulte adjudicatario de la presente contratación.

La documentación solicitada en el presente pliego deberá ser presentada siguiendo las exigencias establecidas en el Pliego de Condiciones Particulares (PCP).

3.6 ESPECIFICACIONES PARA LA PRESENTACIÓN DE PROPUESTAS ECONÓMICAS

Las ofertas de precio podrán ser efectuadas en moneda de curso legal en la República Argentina (PESOS) o en DÓLARES ESTADOUNIDENSES, indicando por separado la suma correspondiente al Impuesto al Valor Agregado (IVA) y la alícuota correspondiente.

SOFSA no reconocerá ni pagará montos derivados de omisiones o por conceptos no incluidos en la OFERTA. Se entenderá que todo lo que haya sido incluido en la OFERTA TÉCNICA y no sea cotizado expresamente en la Planilla de Cotización adjunta será proporcionado sin costo alguno.

3.7. CONSIDERACIONES DE SEGURIDAD INFORMÁTICA

La información relacionada con la configuración y administración de los equipos, software y licencias mencionadas en el presente pliego se clasificará como "Información Confidencial". Se requerirá que el OFERENTE mapee esta clasificación a su propio esquema interno, asegurando que los controles de seguridad sean aplicados adecuadamente.

El OFERENTE deberá cumplir con todas las normativas y leyes vigentes en materia de protección de datos personales, derechos de propiedad intelectual y seguridad de la información. Se establece que cualquier software, firmware o hardware proporcionado deberá cumplir con las licencias y acuerdos de uso correspondientes.

Se deberán definir los controles de acceso a la información, asegurando que solo el personal autorizado pueda acceder a los sistemas y servicios incluidos en este pliego. Asimismo, el OFERENTE deberá proveer a SOFSA una lista detallada del personal autorizado y cumplir con los procedimientos de autorización y retiro de accesos según las políticas de seguridad de la compañía.

En caso de un incidente de seguridad informática, como una violación de datos, intento de acceso no autorizado o interrupción de servicio, el OFERENTE deberá notificar inmediatamente a SOFSA y colaborar con las acciones de mitigación necesarias. Será obligatorio contar con un protocolo de gestión de incidentes que contemple la notificación, análisis y resolución de los mismos dentro de los tiempos de respuesta acordados.

SOFSA tendrá el derecho de llevar a cabo auditorías periódicas sobre los procesos de instalación, mantenimiento y actualización de los servicios contratados. Estas auditorías podrán incluir la revisión de registros de actividad, la evaluación de los controles de seguridad aplicados y la verificación del cumplimiento de las políticas de seguridad establecidas. El OFERENTE deberá proporcionar acceso a la documentación requerida y cooperar plenamente durante estas auditorías.

El OFERENTE deberá garantizar que el personal involucrado en la ejecución del contrato haya recibido capacitación en procedimientos de seguridad de la información, con especial énfasis en gestión de incidentes, control de accesos y protección de datos. Además, en caso de subcontratación de servicios,

el OFERENTE deberá asegurarse de que los terceros involucrados cumplan con las mismas políticas y controles de seguridad exigidos por SOFSA.

Los recursos de computación utilizados para el almacenamiento de respaldos deberán alojarse en centros de datos que cumplan con estándares de seguridad y gestión de riesgos adecuados. Se implementarán controles de seguridad perimetral, registros de auditoría, cifrado de datos en tránsito y en reposo, y autenticación multifactor para accesos administrativos.

El OFERENTE deberá presentar periódicamente informes sobre la efectividad de los controles de seguridad implementados. SOFSA se reserva el derecho de solicitar ajustes y mejoras en las medidas de seguridad en caso de identificarse vulnerabilidades o deficiencias en el cumplimiento de los requisitos de seguridad.

3.8. CERTIFICACIÓN

El servicio se certificará el 100% (CIEN POR CIENTO) al inicio del periodo de vigencia de las licencias.

3.9. ADJUDICACIÓN

La adjudicación será POR LA TOTALIDAD DE LOS RENGLONES de conformidad con las pautas establecidas en el presente documento y NO se aceptarán ofertas parciales.

ANEXO A – PLANILLA DE COTIZACIÓN

ANEXO A - PLANILLA COTIZACIÓN						
Contratación N°:					DETALLE PROVEEDOR	
Clase de Contratación:					Razón Social	
Expediente:					C.U.I.T.	
Objeto:	PROVISIÓN DE SOPORTE PARA FIREWALL DE NUEVA GENERACION Y SISTEMA DE GESTION DE EVENTOS DE SEGURIDAD					
Adjudicación :	Total					
Renglón	**Cantidad**	**U/M**	**Descripción**	**MONEDA**	**Precio Unitario**	**Subtotal (Cantidad x Precio Unitario)**
1	1	C/U	NGFW- Suscripción con Fortinet			
2	1	C/U	SIEM FORTISIEM - Suscripción con Fortinet			
				Subtotal		**0,00**
				I.V.A.		**0,00**
				TOTAL		**0,00**

TRENES ARGENTINOS OPERACIONES

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Hoja Adicional de Firmas
Pliego Especificaciones Tecnicas

Número: IF-2025-101143156-APN-GSYP#SOFSE

CIUDAD DE BUENOS AIRES
Jueves 11 de Septiembre de 2025

Referencia: PET- PROVISIÓN DE SOPORTE PARA FIREWALL DE NUEVA GENERACION Y SISTEMA DE GESTION DE EVENTOS DE SEGURIDAD

El documento fue importado por el sistema GEDO con un total de 10 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.09.11 13:04:10 -03:00

Ariel Juan Cherti
Gerente
Gerencia Sistemas y Procesos
Operadora Ferroviaria Sociedad del Estado

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.09.11 13:04:11 -03:00