TRENES ARGENTINOS
OPERACIONES

Ministerio de Transporte
Presidencia de la Nación

P.E.T

PLIEGO DE ESPECIFICACIONES TECNICAS

"ADQUISICION DE BIENES Y SERVICIOS CONEXOS DE TECNOLOGIAS DE SEGURIDAD INFORMÁTICA"

Artículo 1°. INTRODUCCIÓN

El presente Pliego de Especificaciones Técnicas tiene por objeto establecer las bases y condiciones a las que se ajustará la contratación de la **ADQUISICION DE BIENES Y SERVICIOS CONEXOS DE TECNOLOGIAS DE SEGURIDAD INFORMÁTICA** de la Operadora Ferroviaria S.E., en adelante denominada indistintamente "Trenes Argentinos" o la "Empresa".

La Operadora Ferroviaria Sociedad del Estado (SOFSE) requiere la adquisición de bienes y servicios especializados que permitan aumentar el nivel de seguridad de la información de Trenes Argentinos.

En tal sentido, se encuentran comprendidos dentro del alcance de la contratación, los siguientes ítems:

1.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

- Adquisición de la plataforma y licenciamiento de un sistema reconocido en el mercado de protección de redes con características de *Next Generation Firewall* (NGFW) para la seguridad de la información perimetral que incluya filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", componiendo una plataforma de seguridad integrada y robusta (preferentemente del tipo *appliance* físico).
- Licenciamiento (100 usuarios) para el ingreso remoto con doble factor de autenticación mediante VPN, para uso de la Gerencia de Sistemas y Procesos.

1.2 Ítem B (Servicios de implementación y soporte del firewall de nueva generación (ngfw)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Provisión de servicios conexos para brindar capacitaciones sobre el uso de la herramienta.
- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

1.3 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

- Adquisición de una plataforma de hardware y software que permita proteger las aplicaciones web (de marca F5), teniendo una capacidad de soportar al menos 10 Gb de tráfico de red (L4/L7).
- Adquisición de licencias del software.

1.4 Ítem D (Servicios de implementación y soporte del firewall de aplicaciones web (waf)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Implementación de 10 servicios web a proteger.
- Implementación de perfil de DOS Protection.

- Implementación de perfil de BOT Defense.
- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

1.5 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

- Adquisición de la plataforma y licenciamiento de un sistema reconocido en el mercado de gestión de eventos e información de seguridad (SIEM), que incluya todos los elementos software y hardware necesarios para la recolección, análisis y almacenamiento de eventos.

1.6 Ítem F (Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Implementación de la recolección de eventos sobre 175 dispositivos.
- Provisión de servicios conexos para brindar capacitaciones sobre el uso de la herramienta.
- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

1.7 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:

AD: Active Directory, Directorio Activo que brinda información de autorización de acceso a los usuarios.

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

AyF: Área de Administración y Finanzas.

AyL: Área de Abastecimiento y Logística.

COM: Área de Comercial.

HCM: Área de Recursos Humanos.

PMO: oficina de Administración de Proyectos.

ERP: Para referirse al Sistema Administrativo Integrado (Enterprise Resource Planning) implementado por SOFSE.

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

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.

NGFW: es Firewall de Nueva Generación (NGFW) cuya función es supervisar, filtrar o bloquear el tráfico de red no autorizado.

WAF: es Firewall de Web (WAF) cuya función es la de supervisar, filtrar o bloquear el tráfico HTTP hacia y desde una aplicación web.

HA: Alta disponibilidad.

XSS. (Cross-site scripting o Secuencias de comandos entre sitios): es un ataque que es utilizado para robar información delicada, secuestrar sesiones de usuario, y comprometer el navegador. Esta situación es causada cuando no se validan correctamente los datos de entrada que son usados, o no sanear la salida para su presentación como página web.

Inyección SQL: El objetivo es el de insertar o "inyecta" de código (el más común es el SQL) dentro de la aplicación WEB con el fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de comandos en la base de datos. Con el fin de obtener más información de la requerida.

CSRF (Cross-site request forgery o falsificación de petición de sitios cruzados) Es un ataque malicioso a un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esto explota la confianza que un sitio tiene en un usuario en particular.

Artículo 2°. OBJETO

El objeto de la presente contratación refiere a la adquisición y servicios conexos, bajo la modalidad "llave en mano", correspondientes a los bienes y servicios que se detallan a continuación:

2.1.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

- Adquisición de la plataforma y licenciamiento de un sistema reconocido en el mercado de protección de redes con características de *Next Generation Firewall* (NGFW) para la seguridad de la información perimetral que incluya filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", componiendo una plataforma de seguridad integrada y robusta (preferentemente del tipo *appliance* físico).
- Licenciamiento (100 usuarios) para el ingreso remoto con doble factor de autenticación mediante VPN, para uso de la Gerencia de Sistemas y Procesos.

SOFSE requiere la provisión de una plataforma con tecnología de firewall de nueva generación que aumente el nivel de seguridad de la organización y proteja contra ciber ataques, a instalarse en la infraestructura existente en el centro de procesamiento de datos ARSAT y que sea de ALTA disponibilidad, es decir, redundante a fallos.

Asimismo, debe contar un módulo o solución de análisis y reporte preferentemente separado de la solución principal, que ayude a analizar los eventos más importantes que se generan en el firewall de nueva generación.

El licenciamiento es de tipo permanente o bien como suscripción anual cuya infraestructura deberá instalarse en ARSAT. Debe prever la instalación y puesta en marcha de la infraestructura y entornos de TI del software.

La solución propuesta por el oferente deberá incorporar todo el software y licenciamiento necesario para su funcionamiento (por ej. base de datos, run-time de productos, proyecto con la propuesta de implementación, etc.), ser escalable según los requerimientos de SOFSE.

La entrega final del equipo deberá consensuarse con personal de SOFSE y el lugar de recepción será el centro de procesamiento de datos de ARSAT, ubicado en Benavídez, provincia de Buenos Aires. Asimismo, deberá incluir todos los cables de energía necesarios (C13/C14) y contar con las guías y tornillos para su instalación en el rack.

El alcance de los requerimientos funcionales y técnicos a ser cubiertos por la tecnología propuesta por el oferente se encuentra descriptos en la sección **3.1 Capacidades y antecedentes del oferente**.

2.1.2 Ítem B (Servicios de implementación y soporte del firewall de nueva generación (ngfw)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Provisión de servicios conexos para brindar capacitaciones sobre el uso de la herramienta.

- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

El OFERENTE deberá destinar los recursos de personal necesarios para la instalación, implementación y puesta en marcha de la infraestructura y entornos de TI. Durante la implementación, suministrará soporte técnico en aspectos tales como, configuración, utilización de las herramientas provistas, ajustes de procesos y resolverá aquellos inconvenientes que se deban solucionar. Asimismo, aportará los recursos profesionales con los conocimientos y, fundamentalmente, con la experiencia acorde a lo solicitado. Deberá presentar la conformación del equipo de trabajo y su organigrama, indicando también la cantidad de recursos y tareas que realizarán.

El ADJUDICATARIO generará documentación relacionada con aquellos aspectos técnicos de herramientas, configuración y ajustes que a criterio de SOFSE sean necesarios para el mantenimiento de la solución. El alcance de la documentación será definido por SOFSE.

El ADJUDICATARIO deberá garantizar, durante la vigencia del contrato, el correcto funcionamiento de la solución objeto de la presente contratación y la inmediata resolución de las eventuales fallas durante el período de post-implementación.

El ADJUDICATARIO deberá proveer un período de sesenta (60) días de instalación y operación del equipo, a partir de la entrega final del mismo en carácter de garantía técnica. Es de mencionar que la garantía técnica deberá tener vigencia durante el periodo de implementación y operación establecido en el presente pliego técnico.
El proveedor deberá presentar un plan de transferencia de conocimiento de todo lo que involucra las tareas que se realizan para que en un plazo de 4 meses el equipo de SOFSE se haga responsable del soporte.

Se espera que el ADJUDICATARIO realice la propuesta del servicio de Soporte Post Implementación de acuerdo de nivel de servicio teniendo en cuenta las mejores prácticas del mercado. Los tiempos de respuesta máximos serán:

Prioridad	Tiempo de Respuesta	Detalle
Crítico	2hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas básicas necesarias y esenciales de las operaciones del negocio.
Alto	4hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas diarias de las operaciones del negocio.
Medio	8hs	Las aplicaciones o servicios están funcionando, pero el problema causa un impacto parcial y algunos servicios no funcionan.
Bajo	16hs	Las aplicaciones o servicios se encuentran en funcionamiento. El problema causa un impacto limitado. El servicio que no funciona no es crítico para el negocio y se puede continuar la operación.

Los niveles de servicio se miden dentro del horario contratado. En los casos de prioridad Crítica se requiere que el ADJUDICATARIO trabaje hasta dejar operativo la aplicación afectada.

Debe considerar la disponibilidad de una MESA DE AYUDA en horario administrativo de lunes a viernes de 9 a 18 horas, en modalidad remota, y en caso de ser necesario, guardias para procesos críticos. El contacto será por medio de la MESA DE AYUDA de SOFSE, para facilitar la atención de las solicitudes de usuarios. Es de mencionar que toda la gestión se realizará mediante la herramienta de *Service Desk* de SOFSE.

Los tiempos de respuesta, a los efectos de calcular el nivel de servicio, serán medidos y contados a partir de que el incidente es transferido al grupo resolutor del ADJUDICATARIO por SOFSE ante el incidente, evento o requerimiento detectado y la confirmación de la prueba exitosa de la solución definitiva o alternativa en el entorno de desarrollo, por parte del responsable de aplicaciones de SOFSE. Las horas se computarán durante el horario de servicio (9 a 18 horas).

Si el ADJUDICATARIO incurre en retraso injustificado en la ejecución de las prestaciones, SOFSE aplicará una penalidad. Para ello se basará en la información registrada en la herramienta antes mencionada (*Service Desk*). El incumplimiento de los acuerdos de niveles de servicio (SLA) comprometidos por el ADJUDICATARIO será sancionado con multas.

Penalidades por Incumplimiento de SLA

Se aplicarán las penalidades según lo establecido en la normativa de SOFSE (Artículo 66 del RCC y el capítulo XVII del PBCG)

Estas penalidades serán deducidas de las certificaciones presentadas mensualmente por el pago del servicio de utilización y soporte.

Garantía Técnica

El ADJUDICATARIO está obligado a otorgar una Garantía Técnica por fallas de adaptación, provisión de componentes y/o su implementación sin costo alguno para SOFSE, por el plazo de 12 meses para cada entrega Parcial o Final luego de realizado el Protocolo de Aceptación para la entrega que se trate. Si durante el Plazo de Garantía Técnica, el Organismo Contratante detectara una falla, el Adjudicatario deberá atender el reclamo en un plazo no mayor a 10 días y proceder a su resolución en un tiempo máximo de 30 días. Resuelta la falla, la misma contará con un Periodo de Garantía Técnica Parcial de 6 Meses. En caso de que esto no ocurriese, SOFSE podrá reclamar el pago de penalidades u otras acciones contempladas en este Pliego.

2.1.3 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

- Adquisición de una plataforma de hardware y software que permita proteger las aplicaciones web (de marca F5 Networks), teniendo una capacidad de soportar al menos 10 Gb de tráfico de red (L4/L7).
- Adquisición de licencias del software.

SOFSE tiene implementado en su infraestructura de ARSAT la solución de *F5 Network BIG-IP i2600 Advanced Web Application Firewall (appliance* físico*)*. En la presente contratación se requiere una solución de la misma marca, pero con mejores prestaciones que la mencionada para poder implementar ambas en alta disponibilidad, es decir, redundante a fallos.

El licenciamiento es de tipo permanente o bien como suscripción anual cuya infraestructura deberá instalarse en el centro de procesamiento de ARSAT. Debe prever la instalación y puesta en marcha de la infraestructura y entornos de TI del software.

La solución propuesta por el oferente deberá incorporar todo el software y licenciamiento necesario para su funcionamiento (por ej. base de datos, run-time de productos, proyecto con la propuesta de implementación, etc.), ser escalable según los requerimientos de SOFSE.

La entrega final del equipo deberá consensuarse con personal de SOFSE y el lugar de recepción será el centro de procesamiento de datos de ARSAT, ubicado en Benavídez, provincia de Buenos Aires. Asimismo, deberá incluir todos los cables de energía necesarios (C13/C14) y contar con las guías y tornillos para su instalación en el rack.

El alcance de los requerimientos funcionales y técnicos a ser cubiertos por la tecnología propuesta por el oferente se encuentra descriptos en la **sección 3.1 Capacidades y antecedentes del oferente**.

2.1.4 Ítem D (Servicios de implementación y soporte del firewall de aplicaciones web (waf)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Implementación de 10 servicios web a proteger.
- Implementación de perfil de DOS Protection.
- Implementación de perfil de BOT Defense.
- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

El OFERENTE deberá destinar los recursos de personal necesarios para la instalación, implementación y puesta en marcha de la infraestructura y entornos de TI. Durante la implementación, suministrará soporte técnico en aspectos tales como, configuración, utilización de las herramientas provistas, ajustes de procesos y resolverá aquellos inconvenientes que se deban solucionar. Asimismo, aportará los recursos profesionales con los conocimientos y, fundamentalmente, con la experiencia acorde a lo solicitado. Deberá presentar la conformación del equipo de trabajo y su organigrama, indicando también la cantidad de recursos y tareas que realizarán.

El ADJUDICATARIO generará documentación relacionada con aquellos aspectos técnicos de herramientas, configuración y ajustes que a criterio de SOFSE sean necesarios para el mantenimiento de la solución. El alcance de la documentación será definido por SOFSE.

El ADJUDICATARIO deberá garantizar, durante la vigencia del contrato, el correcto funcionamiento de la solución objeto de la presente contratación y la inmediata resolución de las eventuales fallas durante el período de post-implementación.

El ADJUDICATARIO deberá proveer un período de treinta (30) días de instalación y operación del equipo, a partir de la entrega final del mismo en carácter de garantía técnica. Es de mencionar que la garantía técnica deberá tener vigencia durante el periodo de implementación y operación establecido en el presente pliego técnico.
El proveedor deberá presentar un plan de transferencia de conocimiento de todo lo que involucra las tareas que se realizan para que en un plazo de 4 meses el equipo de SOFSE se haga responsable del soporte.

Se espera que el ADJUDICATARIO realice la propuesta del servicio de Soporte Post Implementación de acuerdo de nivel de servicio teniendo en cuenta las mejores prácticas del mercado. Los tiempos de respuesta máximos serán:

Prioridad	Tiempo de Respuesta	Detalle
Crítico	2hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas básicas necesarias y esenciales de las operaciones del negocio.
Alto	4hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas diarias de las operaciones del negocio.
Medio	8hs	Las aplicaciones o servicios están funcionando, pero el problema causa un impacto parcial y algunos servicios no funcionan.
Bajo	16hs	Las aplicaciones o servicios se encuentran en funcionamiento. El problema causa un impacto limitado. El servicio que no funciona no es crítico para el negocio y se puede continuar la operación.

Los niveles de servicio se miden dentro del horario contratado. En los casos de prioridad Crítica se requiere que el ADJUDICATARIO trabaje hasta dejar operativo la aplicación afectada.

Debe considerar la disponibilidad de una MESA DE AYUDA en horario administrativo de lunes a viernes de 9 a 18 horas, en modalidad remota, y en caso de ser necesario, guardias para procesos críticos. El contacto será por medio de la MESA DE AYUDA de SOFSE, para facilitar la atención de las solicitudes de usuarios. Es de mencionar que toda la gestión se realizará mediante la herramienta de *Service Desk* de SOFSE.

Los tiempos de respuesta, a los efectos de calcular el nivel de servicio, serán medidos y contados a partir de que el incidente es transferido al grupo resolutor del ADJUDICATARIO por SOFSE ante el incidente, evento o requerimiento detectado y la confirmación de la prueba exitosa de la solución definitiva o alternativa en el entorno de desarrollo, por parte del responsable de aplicaciones de SOFSE. Las horas se computarán durante el horario de servicio (9 a 18 horas).

Si el ADJUDICATARIO incurre en retraso injustificado en la ejecución de las prestaciones, SOFSE aplicará una penalidad. Para ello se basará en la información registrada en la herramienta antes mencionada (*Service Desk*). El incumplimiento de los acuerdos de niveles de servicio (SLA) comprometidos por el ADJUDICATARIO será sancionado con multas.

Penalidades por Incumplimiento de SLA

Se aplicarán las penalidades según lo establecido en la normativa de SOFSE (Artículo 66 del RCC y el capítulo XVII del PBCG)

Estas penalidades serán deducidas de las certificaciones presentadas mensualmente por el pago del servicio de utilización y soporte.

Garantía Técnica

El ADJUDICATARIO está obligado a otorgar una Garantía Técnica por fallas de adaptación, provisión de componentes y/o su implementación sin costo alguno para SOFSE, por el plazo de 12 meses para cada entrega Parcial o Final luego de realizado el Protocolo de Aceptación para la entrega que se trate. Si durante el Plazo de Garantía Técnica, el Organismo Contratante detectara una falla como las que se describen en el párrafo Anterior, el Adjudicatario deberá atender el reclamo en un plazo no mayor a 10 días y proceder a su resolución en un tiempo máximo de 30 días. Resuelta la falla, la misma contará con un Periodo de Garantía Técnica Parcial de 6 Meses. En caso de que esto no ocurriese, SOFSE podrá reclamar el pago de penalidades u otras acciones contempladas en este Pliego.

2.1.5 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

- Adquisición de la plataforma y licenciamiento de un sistema reconocido en el mercado de gestión de eventos e información de seguridad (SIEM), que incluya todos los elementos necesarios para la recolección, análisis y almacenamiento de eventos.

SOFSE requiere de una herramienta principal de monitoreo y correlación de eventos de seguridad para ser implementada en ARSAT, que además de contar con capacidades para la prevención y detección temprana de amenazas e incidentes, análisis de vulnerabilidades técnicas, y análisis y resolución de incidentes de seguridad (todo ello de forma centralizada y con procesos y procedimientos operativos de seguridad consistentes), debe permitir generar reportes efectivos sobre el estado global de la seguridad y sus riesgos.

La solución debe contener un catálogo de reglas de correlación que permita detectar anomalías y realizar el análisis automatizado de la información en tiempo real, generando alertas 24x7. Asimismo, debe clasificar los ataques y amenazas detectados en función de su criticidad y/o prioridad. Asimismo, debe permitir:

- Disponer en tiempo real de análisis de información, mediante un procesamiento avanzado de registros de auditorías (logs) y la correlación de eventos en tiempo real, que permitan apoyar tanto la operación de sistemas y servicios como la gestión de las obligaciones legales de custodia de evidencias y comunicación de incidentes en los plazos establecidos.
- Realizar un descubrimiento de dispositivos y mantener una base de datos de configuraciones (CMDB), mediante técnicas de auto-descubrimiento y aprendizaje de activos y mapeos inter-relacionales, en entornos tanto físico como virtuales y de cloud, de aplicaciones, usuarios, y dispositivos. En este sentido, la solución ofertada deberá tener CMDB nativa dentro de la propia herramienta de SIEM.
- Arquitectura escalable, con capacidad de operación tanto en entornos de datacenter como cloud, con almacenaje de eventos No SQL, y correlación distribuida de eventos en tiempo real (patentada).
- Capacidad de monitorización de rendimiento y disponibilidad por SNMP y WMI.
- Integraciones rápidas de tecnologías y casos de uso pre configurados para dispositivos físicos y virtuales.
- Posibilidad de incorporar indicadores de compromiso para incrementar el nivel de seguridad en la correlación de eventos.
- Correlación de eventos SOC/NOC, para disponer en un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:
    - Rendimiento y disponibilidad.
    - CPU, memoria y almacenamiento.
    - Detección de cambios de configuración.
    - Cuadros de mando dinámicos.

El licenciamiento es de tipo permanente o bien como suscripción anual cuya infraestructura deberá instalarse en ARSAT. Debe prever la instalación y puesta en marcha de la infraestructura y entornos de TI del software.

La solución propuesta por el oferente deberá incorporar todo el software y licenciamiento necesario para su funcionamiento (por ej. base de datos, run-time de productos, proyecto con la propuesta de implementación, etc.), ser escalable según los requerimientos de SOFSE, y debe considerar que la misma se integrará a una estructura de virtualización a ser hospedada en ARSAT.

Las versiones de sistema operativo donde va a operar la solución en ARSAT son:

- Microsoft Windows 2012R2 o superior
- Debian 9 o superior
- Centos 7 o superior
- Ubuntu 18.04 o superior
- Red Hat Enterprise Linux 7.0 o superior

Asimismo, se requiere que el almacenamiento centralizado de todos los registros de auditoría recopilados sea independiente a la base de datos utilizada por el sistema gestor.

El alcance de los requerimientos funcionales y técnicos a ser cubiertos por la tecnología propuesta por el oferente se encuentra descriptos en la sección **3.1 Capacidades y antecedentes del oferente**.

2.1.6 Ítem F (Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)):

- Provisión de servicios conexos para la instalación, implementación, puesta en marcha y optimización de la infraestructura y entornos de TI del software durante el proyecto.
- Implementación de la recolección de eventos sobre 175 dispositivos.
- Provisión de servicios conexos para brindar capacitaciones sobre el uso de la herramienta.
- Provisión de servicios conexos para el soporte post implementación del software e infraestructura relacionada, y soporte a usuarios.

El OFERENTE deberá destinar los recursos de personal necesarios para la instalación, implementación y puesta en marcha de la infraestructura y entornos de TI. Durante la implementación, suministrará soporte técnico en aspectos tales como, configuración, utilización de las herramientas provistas, ajustes de procesos y resolverá aquellos inconvenientes que se deban solucionar. Asimismo, aportará los recursos profesionales con los conocimientos y, fundamentalmente, con la experiencia acorde a lo solicitado. Deberá presentar la conformación del equipo de trabajo y su organigrama, indicando también la cantidad de recursos y tareas que realizarán.

El ADJUDICATARIO generará documentación relacionada con aquellos aspectos técnicos de herramientas, configuración y ajustes que a criterio de SOFSE sean necesarios para el mantenimiento de la solución. El alcance de la documentación será definido por SOFSE.

El ADJUDICATARIO deberá garantizar, durante la vigencia del contrato, el correcto funcionamiento de la solución objeto de la presente contratación y la inmediata resolución de las eventuales fallas durante el período de post-implementación.

El ADJUDICATARIO deberá proveer un período de treinta (90) días de instalación y operación del equipo, a partir de la entrega final del mismo en carácter de garantía técnica. Es de mencionar que la garantía técnica deberá tener vigencia durante el periodo de implementación y operación establecido en el presente pliego técnico.
El proveedor deberá presentar un plan de transferencia de conocimiento de todo lo que involucra las tareas que se realizan para que en un plazo de 4 meses el equipo de SOFSE se haga responsable del soporte.

Se espera que el ADJUDICATARIO realice la propuesta del servicio de Soporte Post Implementación de acuerdo de nivel de servicio teniendo en cuenta las mejores prácticas del mercado. Los tiempos de respuesta máximos serán:

Prioridad	Tiempo de Respuesta	Detalle
Crítico	2hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas básicas necesarias y esenciales de las operaciones del negocio.
Alto	4hs	Las aplicaciones o servicios no se encuentran en funcionamiento. El problema no permite cumplir con tareas diarias de las operaciones del negocio.
Medio	8hs	Las aplicaciones o servicios están funcionando, pero el problema causa un impacto parcial y algunos servicios no funcionan.
Bajo	16hs	Las aplicaciones o servicios se encuentran en funcionamiento. El problema causa un impacto limitado. El servicio que no funciona no es crítico para el negocio y se puede continuar la operación.

Los niveles de servicio se miden dentro del horario contratado. En los casos de prioridad Crítica se requiere que el ADJUDICATARIO trabaje hasta dejar operativo la aplicación afectada.

Debe considerar la disponibilidad de una MESA DE AYUDA en horario administrativo de lunes a viernes de 9 a 18 horas, en modalidad remota, y en caso de ser necesario, guardias para procesos críticos. El contacto será por medio de la MESA DE AYUDA de SOFSE, para facilitar la atención de las solicitudes de usuarios. Es de mencionar que toda la gestión se realizará mediante la herramienta de *Service Desk* de SOFSE.

Los tiempos de respuesta, a los efectos de calcular el nivel de servicio, serán medidos y contados a partir de que el incidente es transferido al grupo resolutor del ADJUDICATARIO por SOFSE ante el incidente, evento o requerimiento detectado y la confirmación de la prueba exitosa de la solución definitiva o alternativa en el entorno de desarrollo, por parte del responsable de aplicaciones de SOFSE. Las horas se computarán durante el horario de servicio (9 a 18 horas).

Si el ADJUDICATARIO incurre en retraso injustificado en la ejecución de las prestaciones, SOFSE aplicará una penalidad. Para ello se basara en la información registrada en la herramienta antes mencionada (*Service Desk*). El incumplimiento de los acuerdos de niveles de servicio (SLA) comprometidos por el ADJUDICATARIO será sancionado con multas.

Penalidades por Incumplimiento de SLA

Se aplicarán las penalidades según lo establecido en la normativa de SOFSE (Artículo 66 del RCC y el capítulo XVII del PBCG)

Estas penalidades serán deducidas de las certificaciones presentadas mensualmente por el pago del servicio de utilización y soporte.

Garantía Técnica

El ADJUDICATARIO está obligado a otorgar una Garantía Técnica por fallas de adaptación, provisión de componentes y/o su implementación sin costo alguno para SOFSE, por el plazo de 12 meses para cada entrega Parcial o Final luego de realizado el Protocolo de Aceptación para la entrega que se trate. Si durante el Plazo

de Garantía Técnica, el Organismo Contratante detectara una falla como las que se describen en el párrafo Anterior, el Adjudicatario deberá atender el reclamo en un plazo no mayor a 10 días y proceder a su resolución en un tiempo máximo de 30 días. Resuelta la falla, la misma contará con un Periodo de Garantía Técnica Parcial de 6 Meses. En caso de que esto no ocurriese, SOFSE podrá reclamar el pago de penalidades u otras acciones contempladas en este Pliego.

2.2 Estructura organizativa y gobierno del proyecto

Equipo de trabajo del ADJUDICATARIO

Responsabilidades:

El ADJUDICADO deberá destinar los recursos de personal necesarios para la concreción de los objetivos esperados.

2.3 Planificación y ejecución del proyecto

2.3.1 Plazo de ejecución

Para la provisión del servicio, el ADJUDICATARIO dispondrá del siguiente plazo para su ejecución:

2.3.1.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

El plazo de entrega es de CUATRO (4) meses para la adquisición, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio. El plazo de la vigencia de las licencias y soporte con el fabricante se establece en VEINTICUATRO (24) meses, con posibilidades de renovación.

2.3.1.2 Ítem B (Servicios de implementación y soporte del firewall de nueva generación (ngfw)):

El plazo para la ejecución del servicio se establece de VEINTICUATRO (24) meses, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio.

2.3.1.3 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

El plazo de entrega es de CUATRO (4) meses, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio. El plazo de la vigencia de las licencias y soporte con el fabricante se establece en VEINTICUATRO (24) meses, con posibilidades de renovación.

2.3.1.4 Ítem D (Servicios de implementación y soporte del firewall de aplicaciones web (waf)):

El plazo para la ejecución del servicio se establece de VEINTICUATRO (24) meses, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio.

2.3.1.5 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

El plazo de entrega es de CUATRO (4) meses, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio. El plazo de la vigencia de las licencias y soporte con el fabricante se establece en VEINTICUATRO (24) meses, con posibilidades de renovación.

2.3.1.6 Ítem F (Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)):

El plazo para la ejecución del servicio se establece de VEINTICUATRO (24) meses, comenzando a contabilizar a partir de la suscripción del acta de inicio del servicio.

2.3.2 Entregables

Para la provisión del servicio el ADJUDICATARIO deberá desarrollar y generar los entregables definidos, pudiendo adicionar cualquier otro que considere oportuno:

2.3.2.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

HITO 1
Entrega de equipamiento, licencias y contratos de soporte con el fabricante

- Entrega de equipamiento.
- Adquisición de licencias y contratos de soporte con el fabricante.

2.3.2.2 Ítem B (Servicios de implementación y soporte del firewall de nueva generación (ngfw)):

HITO 1
Instalación y configuración del entorno

- Acta de constitución del PROYECTO.
- Documento detallado del alcance del PROYECTO.
- Infraestructura del PROYECTO.
- Documentación de entornos.
- Definición de requerimientos de infraestructura.

- Puesta en marcha de infraestructura.
- Configuración de la solución.
- Especificaciones técnicas.
- Preparación de datos de prueba.
- Planificación pruebas unitarias.

HITO 2
Implementación y entrenamiento del producto

- Puesto en producción de la solución.
- Entrenamiento a usuarios finales posterior a salida en vivo.
- Cierre de Fase/PROYECTO.

HITO 3
Servicio de soporte y atención de incidentes (24 meses)

- Diagnóstico de la calidad de la fase de soporte post implementación.
- Resolución incidentes post-implementación.
- Plan de servicios y plan de actividades realizadas y a realizar del soporte.
- Reporte ejecutivo mensual basado en resultados del plan general.
- Plan de transferencia de conocimiento al personal de SOFSE y documentación que soporte el mismo.

2.3.2.3 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

HITO 1
Entrega de equipamiento, licencias y contratos de soporte con el fabricante

- Entrega de equipamiento.
- Adquisición de licencias y contratos de soporte con el fabricante.

2.3.2.4 Ítem D (Servicios de implementación y soporte del firewall de aplicaciones web (waf)):

HITO 1
Instalación y configuración del entorno

- Acta de constitución del PROYECTO.
- Documento detallado del alcance del PROYECTO.
- Infraestructura del PROYECTO.
- Documentación de entornos.
- Definición de requerimientos de infraestructura.
- Puesta en marcha de infraestructura.
- Configuración de la solución.
- Especificaciones técnicas.
- Preparación de datos de prueba.
- Planificación pruebas unitarias.

HITO 2
Implementación y entrenamiento del producto

- Puesto en producción de la solución.
- Implementación de 10 servicios web a proteger.
- Implementación de perfil de DOS Protection.
- Implementación de perfil de BOT Defense.
- Entrenamiento a usuarios finales posterior a salida en vivo.
- Cierre de Fase/PROYECTO.

HITO 3
Servicio de soporte y atención de incidentes (24 meses)

- Diagnóstico de la calidad de la fase de soporte post implementación.
- Resolución incidentes post-implementación.
- Plan de servicios y plan de actividades realizadas y a realizar del soporte.
- Reporte ejecutivo mensual basado en resultados del plan general.
- Plan de transferencia de conocimiento al personal de SOFSE y documentación que soporte el mismo.

2.3.2.5 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

HITO 1
Entrega de licencias y soporte con el fabricante

- Adquisición de licencias y contratos de soporte con el fabricante.

2.3.2.6 Ítem F (Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)):

HITO 1
Instalación y configuración del entorno

- Acta de constitución del PROYECTO.
- Documento detallado del alcance del PROYECTO.
- Infraestructura del PROYECTO.
- Documentación de entornos.
- Definición de requerimientos de infraestructura.
- Puesta en marcha de infraestructura.
- Configuración de la solución.
- Especificaciones técnicas.
- Preparación de datos de prueba.
- Planificación pruebas unitarias.

HITO 2
Implementación y entrenamiento del producto

- Puesto en producción de la solución.
- Implementación de la recolección de eventos sobre 175 dispositivos.
- Entrenamiento a usuarios finales posterior a salida en vivo.
- Cierre de Fase/PROYECTO.

HITO 3
Servicio de soporte y atención de incidentes (24 meses)

- Diagnóstico de la calidad de la fase de soporte post implementación.
- Resolución incidentes post-implementación.
- Plan de servicios y plan de actividades realizadas y a realizar del soporte.
- Reporte ejecutivo mensual basado en resultados del plan general.
- Plan de transferencia de conocimiento al personal de SOFSE y documentación que soporte el mismo.

2.3.3 Certificaciones de servicios

Certificación de hitos del proyecto y presentación:

A los fines de la certificación de hitos del proyecto, los mismos se regirán de acuerdo con lo siguiente:

2.3.3.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

HITO	Descripción	%
1	Entrega de equipamiento, licencias y soporte con el fabricante	100%

2.3.3.2 Ítem B (Servicios de implementación y soporte del firewall de nueva generación (ngfw)):

HITO	Descripción	%
1	Instalación y configuración del entorno	30%
2	Implementación y entrenamiento del producto	40%
3	Servicio de soporte y atención de incidentes (24 meses)	30%

2.3.3.3 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

HITO	Descripción	%
1	Entrega de equipamiento, licencias y soporte con el fabricante	100%

2.3.3.4 Ítem D (Servicios de implementación y soporte del firewall de aplicaciones web (waf)):

HITO	Descripción	%
1	Instalación y configuración del entorno	30%
2	Implementación y entrenamiento del producto	40%
3	Servicio de soporte y atención de incidentes (24 meses)	30%

2.3.3.5 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

HITO	Descripción	%
1	Entrega de licencias y soporte con el fabricante	100%

2.3.3.6 Ítem F (Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)):

HITO	Descripción	%
1	Instalación y configuración del entorno	30%
2	Implementación y entrenamiento del producto	40%
3	Servicio de soporte y atención de incidentes (24 meses)	30%

2.3.4 Consideraciones generales del servicio

El OFERENTE generará documentación relacionada con aquellos aspectos técnicos de herramientas, configuración y ajustes que a criterio de SOFSE sean necesarios para el mantenimiento de la infraestructura. El alcance de la documentación será definido en conjunto con SOFSE.

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

2.3.5 Lugar de ejecución y ubicación del equipo de trabajo

Las tareas presenciales se realizarán en:

- Ramos Mejía 1398 - CABA
- Bullrich 2 - CABA

- ARSAT - Benavidez

SOFSE podrá modificar en cualquier momento el lugar de ejecución y la ubicación del equipo de trabajo, dentro de los antes mencionados, así como la distribución de los integrantes de los equipos de trabajo entre los mismos.

2.3.6 Situaciones especiales

En casos especiales que impidan realizar tareas y/o reuniones presenciales en las instalaciones de la SOFSE, las mismas se coordinarán en forma remota con herramientas estándar de conectividad por Internet o vía telefónica. El proveedor debe contar con las instalaciones y herramientas necesarias para el desarrollo de las tareas sin costo adicional para SOFSE.

2.3.7 Horario de atención

- Lunes a Viernes hábiles de 9 a 18hs.
- En los casos de reuniones se prevé que los mismos serán en las oficinas de Bullrich 2 y Ramos Mejía 1398 1er Piso.

Artículo 3°. CAPACIDADES DEL OFERENTE Y ESPECIFICACIONES DE PROPUESTAS.

Las siguientes capacidades y especificaciones son aplicables a lo requerido.

3.1 Capacidades y antecedentes del oferente

El OFERENTE deberá:

- Contar con una organización con las capacidades y los antecedentes requeridos.

Presentar experiencia de trabajos comprobables de similar naturaleza a la descripta en el presente pliego, ejecutadas y en ejecución, en los últimos diez (10) 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.

  - En todos los casos el Comitente se reserva el derecho de realizar las constataciones que considere necesarias.
  - Acreditar experiencia comprobable en la utilización de metodología de soporte.

- Disponer de recursos humanos en cantidad y calidad suficientes para sostener en el tiempo el nivel de servicio del soporte solicitado.
- Disponer de recursos técnicos con Certificación Oficial del fabricante vigente, donde se explicite la capacidad del oferente para comercializar la tecnología.
- El oferente deberá acreditar certificación de calidad ISO 9001 en soporte de tecnología informática.

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 SOFSE.

El OFERENTE generará documentación relacionada con aquellos aspectos técnicos de herramientas, configuración y ajustes que a criterio de SOFSE sean necesarios para el mantenimiento de la infraestructura. El alcance de la documentación será definido en conjunto con SOFSE.

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

Es MANDATORIO que el referente técnico del OFERENTE posea experiencia en trabajos similares y resida en Argentina para participar de actividades en sitio presencial en caso de ser requerido por SOFSE.

El OFERENTE aportará los recursos profesionales con los conocimientos y, fundamentalmente, con la experiencia que permitan cumplir con los objetivos del presente PET. En la propuesta, debe adjuntar los CVs de los recursos a presentar en el servicio, especificar dedicación (part-time o full-time) y si son residentes de Argentina.

El adjudicatario aportará los recursos profesionales con los conocimientos y, fundamentalmente, con la experiencia acorde a lo solicitado. La Propuesta Técnica deberá contemplar la conformación del equipo de trabajo y su organigrama, indicando la cantidad de recursos, el detalle de la experiencia de cada uno de los consultores, especificar dedicación (part-time o full-time) y ser residentes de Argentina.

En el caso de tratarse de una Unión Transitoria de Empresas (UTE), la certificación de antecedentes será válida siguiendo las exigencias establecidas en el Pliego de Condiciones Particulares.

Durante el servicio no se podrán cambiar los consultores sin previo acuerdo con SOFSE.

La coordinación de vacaciones o licencias debe ser acordada con SOFSE sin excepción.

Asimismo, el OFERENTE deberá presentar las soluciones tecnológicas que cumplan con las siguientes características:

3.1.1 Ítem A (Adquisición de un firewall de nueva generación (ngfw)):

Generales

(1) Aceleración por Hardware para las funciones de ruteo, firewall y tunelización de tráfico WiFi.
(2) HA activo-pasivo y activo-activo.
(3) La gestión del equipo debe ser posible a través de la interfaz de administración web disponible localmente en el mismo equipo.
(4) IPv6 en forma nativa (manteniendo las mismas características y rendimiento que IPv4).
(5) Soporte a ruteo estático y dinámico (RIP, OSPF v2 y v3, ISIS y BGP).
(6) Soporte a ruteo por política.
(7) Soporte a protocolos de monitoreo como SNMP y sFlow.
(8) Soporte a Syslog, con capacidad de envío mediante TCP y SSL.
(9) Debe permitir la creación de hasta 10 sistemas virtuales en el mismo equipo.
(10) Soporte a VXLAN.
(11) Debe soportar Traffic Shaping con la posibilidad de aplicarlo, por usuario, IP, interface o aplicación detectada.
(12) La solución debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución.
(13) Con el fin de obtener una solución acorde a las necesidades y prevención de amenazas en ciber seguridad más óptima y actualizada, se requiere que la solución propuesta obtenga la calificación de Líder en la Evaluación de Cuadrante Mágico de Gartner para Firewall Empresarial de los últimos 3 años (2019 - 2021).

Firewall:

(14) Debe soportar la creación de zonas.
(15) Aplicación de políticas por zona o interfaces, por usuarios, direcciones IP o tipos de dispositivo.
(16) NAT.
(17) VPN IPSec de sitio a sitio y para acceso remoto (sin límite de licencias).
(18) VPN SSL para acceso remoto.
(19) Protecciones contra DoS (denegación de servicio).
(20) Inspección de trafico SSL (con la capacidad de descifrar el trafico cifrado) entrante y saliente sin necesidad de agregado de soluciones adicionales.
(21) Posibilidad de armar políticas en base a objetos Geográficos.

(22) Base de datos de Servicios de Internet (actualizada dinámicamente) para el uso en políticas de seguridad.
(23) Capacidad de funcionar como proxy web explícito y como proxy transparente en forma simultánea.
(24) Debe permitir la autenticación transparente (SSO) con sistemas de Active Directory.

Requerimientos de Alta Disponibilidad:

(25) La solución debe soportar la configuración de alta disponibilidad activo/pasivo y activo/activo en modo transparente.
(26) La solución debe soportar la configuración de alta disponibilidad activo/pasivo y activo/activo en capa 3.
(27) La configuración de alta disponibilidad debe sincronizar:
- Sesiones.
- Configuraciones.
- Políticas de Firewalls, NAT, QoS y objetos de la red.
- Las asociaciones de seguridad VPN.
- Tablas FIB.

(28) En modo de alta disponibilidad debe permitir la supervisión de fallos de enlace.
(29) La solución debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad.

Requerimientos para la Identificación de usuarios

(30) La solución debe permitir de crear políticas basadas en la identidad del usuario a través de la integración con LDAP, Active Directory, E-directorio, RADIUS y base de datos local.
(31) La solución debe permitir la integración con Microsoft Active Directory para identificar usuarios y grupos.
(32) La solución debe soportar single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.
(33) La solución no debe solicitar re-autenticación de usuario para la utilización de los servicios permitidos según las políticas aplicadas (SSO).
(34) La solución debe permitir la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
(35) La solución debe permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
(36) La solución debe incluir al menos cien (100) Licencias para Autenticación de Múltiple Factor para los usuarios que acceden por VPN.
(37) La solución debe soportar la autenticación de portal cautivo (red de cortesía) mediante protocolo RADIUS y/o LDAP

SDWAN:

A los fines de permitir un óptimo aprovechamiento en el uso simultáneo de los enlaces a Internet y de WAN se requiere que la solución de Firewall incorpore la funcionalidad de SDWAN.

(38) La solución debe soportar SD-WAN de forma nativa.
(39) La solución debe soportar agregar al menos 200 interfaces dentro de SD-WAN.
(40) La solución debe generar un canal de trasporte a través de una red virtual llamada "Red overlay", la cual debe tener independencia de las redes físicas, conocido como "Red underlay".
(41) Soporte a más de 5 vínculos a Internet.
(42) La solución debe realizar cambios automáticamente en el envío de tráfico de acuerdo con los valores de rendimientos (Latencia, Jitter, Packet Loss).
(43) La solución debe soportar enrutamiento de paquetes basado en la aplicación y el rendimiento (Latencia, Jitter, Packet Loss) de los enlaces y el estado de la ruta.
(44) La solución debe soportar la creación de reglas de enrutamiento de enlaces por IP de origen, destino, aplicación, usuarios, grupos de usuarios o servicios conocidos de internet.
(45) La solución debe permitir definir al menos 4 estrategias de enrutamiento distintas dentro de las reglas de SD-WAN.
(46) La solución debe soportar balanceo de enlaces por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces.
(47) Las reglas de SD-WAN deben soportar QoS, shaping de tráfico, ruteo por políticas, IPSEC VPN como interfaces miembros.
(48) La solución debe permitir la utilización de FEC (Forward Error Correction).
(49) La solución debe permitir el balanceo de tráfico por sesiones.
(50) La solución debe permitir el balanceo de tráfico por paquetes dentro de túneles IPSec.
(51) La solución debe permitir la implementación sin asistencia de SD-WAN, es decir, Zero Touch Provisioning.

Control de Aplicaciones:

(52) Control de Aplicaciones en capa 7, para la detección de tráfico sin importar el puerto que utilicen.
(53) Reconocer al menos 3000 aplicaciones diferentes.
(54) Debe inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas independiente de puerto y protocolo que usen.
(55) Debe permitir la creación de firmas de aplicación manuales.
(56) La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP.
(57) Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
(58) Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
(59) Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.

Prevención de Antimalware:

(60) La solución debe incluir firmas de virus y malware con actualización periódica desde una base de datos provista por el fabricante.
(61) La solución debe incluir un motor de antivirus heurístico.
(62) La solución debe permitir realizar escaneos en los siguientes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, CIFS.
(63) La solución debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
(64) La solución debe tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
(65) La solución debe aislar automáticamente las máquinas infectadas de otros segmentos de red.
(66) La solución debe tener protección contra ataques de día cero a través de una estrecha integración con componentes de Sandbox entregado como servicio en la nube.
(67) El servicio de Sandboxing debe contar con la capacidad de analizar hasta 10 muestras por minuto.

Prevención de Explotación de Vulnerabilidades en Sistemas Operativos y Software

(68) La solución debe tener módulo IPS integrado en el propio equipo.
(69) La solución debe incluir firmas de prevención de intrusiones (IPS) y actualización periódica desde una base de datos provista por el fabricante.
(70) Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
(71) La solución debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuarios, grupos de usuarios y la combinación de todos estos elementos.
(72) La solución debe permitir el bloqueo de vulnerabilidades y exploits conocidos.
(73) La solución debe incluir la protección contra ataques de denegación de servicio.
(74) La solución debe proteger la arquitectura mediante análisis de decodificación de protocolo.
(75) La solución debe proteger la arquitectura mediante análisis para detectar anomalías de protocolo.
(76) La solución debe proteger la arquitectura mediante análisis para detectar malformaciones de paquetes.
(77) La solución debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
(78) La solución debe detectar y bloquear los escaneos de puertos de origen.
(79) La solución debe bloquear ataques realizados por gusanos (worms) conocidos.
(80) La solución debe contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
(81) La solución debe poder crear firmas personalizadas en la interfaz gráfica del producto.

(82) La solución debe identificar y bloquear la comunicación con redes de bots mediante firmas de IPS y una base de reputación IP provista, mantenida y actualizada periódicamente por el fabricante.
(83) La solución debe registrar la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
(84) La solución debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
(85) Los eventos deben identificar el país que origino la amenaza.

Filtrado de URL

(86) Tener por lo menos 80 categorías de URL, actualizadas dinámicamente por el fabricante de la solución.
(87) Permitir página de bloqueos personalizados.
(88) Los filtros URL deben poder aplicarse por política de seguridad.
(89) Debe permitir la definición de listas negras y blancas de URL, por tiempo y horario.
(90) Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
(91) Además del Web Proxy explícito, debe soportar proxy web transparente.
(92) Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local.

Identificación de Usuarios

(93) Las políticas de seguridad deben permitir la integración con servicios de Active Directory, LDAP, y base de datos local.
(94) Debe permitir crear reglas por grupos de usuario o usuarios individuales.
(95) Debe tener integración con RADIUS.
(96) Debe incluir portal captivo para autenticación explicita de los usuarios.
(97) Debe soportar métodos de autenticación como NTLM y Kerberos.

DLP

(98) Permite la creación de filtros para archivos (por tipo y tamaño) y datos predefinidos.
(99) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
(100) Soportar la identificación de archivos comprimidos y cifrados.
(101) Permitir identificar y opcionalmente prevenir la transferencia de información sensible

QoS Traffic Shaping

(102) Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
(103) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo.
(104) Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones.
(105) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
(106) En QoS debe permitir la definición de tráfico con ancho de banda garantizado.
(107) En QoS debe permitir la definición de tráfico con máximo ancho de banda.
(108) En QoS debe permitir la definición de colas de prioridad.
(109) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
(110) Soportar marcación de paquetes DiffServ, incluso por aplicación.
(111) Soportar la modificación de los valores de DSCP para Diffserv.
(112) Soportar priorización de tráfico utilizando información de Tipo de Servicio.
(113) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping.
(114) Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Geolocalización

(115) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países.
(116) Debe permitir la visualización de los países de origen y destino en los registros de acceso.
(117) Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN

(118) Soportar VPN de sitio-a-sitio y cliente-a-sitio.
(119) Soportar VPN IPSec, VPN SSL.
(120) La VPN IPSec debe ser compatible con 3DES y AES de 128, 192 y 256 (Advanced Encryption Standard).
(121) La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
(122) La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2),
(123) La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.
(124) Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.

Solución de Análisis y Reportes

Con el fin de lograr una visualización completa de la solución requerida se solicita un sistema que permita recibir los logs de las soluciones de NGFW, y permita ver en un único panel de control las distintas variables destacables de seguridad y rendimiento de la solución mencionada, para que a posteriori permita elaborar reportes estándar y personalizables de acuerdo a los requerimientos:

Generales

(125) Debe soportar acceso vía SSH, WEB (HTTPS) y Telnet para la gestión de la solución.
(126) Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
(127) Permitir acceso simultáneo de administración, así como permitir crear roles y permisos personalizados, segregación de funciones y conexiones simultaneas.
(128) Soporte SNMP versión 2 y 3.
(129) La solución debe contar con un Servicio o Suscripción que permita la visualización de Alertas de cuando se produce un evento tipo "Virus Outbreak" o Alarma General de Virus de afectación Global.
(130) Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
(131) Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
(132) Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH y Telnet.
(133) Autenticación de usuarios de acceso a la plataforma vía Radius.
(134) Generación de informes en tiempo real de tráfico, ya sea en mapas geográficos y en tablas.
(135) Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
(136) Autenticación de usuarios de acceso a la plataforma vía Microsoft Active Directory.
(137) Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
(138) Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
(139) Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.
(140) Contar con mecanismos de borrado automático de logs antiguos.
(141) Permitir la importación y exportación de reportes.
(142) Debe contar con la capacidad de crear informes en formato HTML, PDF, XML, CSV.
(143) Generación de logs de auditoria, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
(144) Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
(145) La solución debe contar con reportes predefinidos.
(146) Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.
(147) Debe ser posible la duplicación de reportes existentes para su posterior edición.
(148) Debe tener la capacidad de personalizar la portada de los reportes obtenidos.

(149) Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
(150) Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
(151) Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
(152) Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
(153) Debe permitir descargar de la plataforma los archivos de logs para uso externo.
(154) Tener la capacidad de generar y enviar reportes periódicos automáticamente.
(155) Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
(156) Permitir el envío por email de manera automática de reportes.
(157) Debe permitir que el reporte a enviar por email sea al destinatario específico.
(158) Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
(159) Debe ser posible visualizar gráficamente en tiempo real el consumo de disco y la tasa de generación de logs por cada dispositivo gestionado.
(160) Debe permitir el uso de filtros en los reportes.
(161) Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
(162) Permitir que los reportes creados sean en idioma Español.
(163) Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
(164) Debe permitir el envío automático de reportes a un servidor externo SFTP, SCP o FTP.
(165) Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para su en gráficas y tablas en reportes.
(166) Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
(167) Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
(168) Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
(169) Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
(170) La solución debe servir como un servidor Syslog y aceptar logs de diferentes fabricantes.
(171) Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
(172) Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
(173) Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos.
(174) Debe permitir visualizar en tiempo real los logs recibidos.

Reportes

(175) Debe permitir la creación de Dashboards personalizados para visualizar tráfico de aplicaciones, categorías de URL, amenazas, servicios, países, origen y destino.
(176) Debe poder contar con un Indicador de Compromisos (IoC), que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
(177) Debe contar con reporte de cumplimiento de PCI DSS.
(178) Debe contar con reporte de utilización de aplicaciones SaaS.
(179) Debe contar con reporte de prevención de perdida de datos (DLP).
(180) Debe contar con reporte de VPN.
(181) Debe contar con reporte de Sistema de prevención de intrusos (IPS).
(182) Debe contar con reporte de reputación de cliente.
(183) Debe contar con reporte de análisis de seguridad de usuario.
(184) Debe contar con reporte de análisis de amenaza cibernética.
(185) Debe contar con reporte de cumplimiento PCI de Wireless.
(186) Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi.
(187) Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
(188) Debe contar con análisis de seguridad y uso de web, si se tiene plataforma de Cache.
(189) Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web.

Licenciamiento y actualizaciones

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.

Desempeño / Conectividad del Equipamiento Firewall (cantidad recomendada: 2)

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad:

Número de Interfaces Requeridas	12x GE RJ45 8x GE SFP 10x GE SFP+ (Proveer 4 Gbics SFP+ FO-SR por equipo) 2x Puertos para HA: SFP+ 10GE 2 x GE RJ45 Puertos administrativos
Throughput de Firewall (con paquetes de 512 Bytes)	180 Gbps
Latencia de firewall (con paquetes de 64 bytes)	4 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	50 Gbps
Throughput de NGFW	10 Gbps

Throughput de Inspección SSL	15 Gbps
Políticas de Firewall admitidas	10.000
Túneles IPsec gateway to gateway	10.000
Túneles IPsec client to gateway	50.000
Túneles SSL	10.000
Throughput VPN SSL	10 Gbps
Sesiones Concurrentes TCP	10 Millones
Inspección Sesiones SSL Concurrentes	1 Millón
Nuevas sesiones / segundo (TCP)	700.000
Inspección sesiones SSL / segundo	9.000
Puntos acceso soportados / AP en modo túnel	4000 / 2000
Switches Soportados	150
Sistemas Virtuales incluidos / Máximo soportado	10/200

Solución de Análisis y Reportes

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad:

Formato de Solución	Virtual Appliance
Almacenamiento Diario de Logs	25 GB
Capacidad de Almacenamiento	10 TB
Cantidad Máxima de Dispositivos Soportados	10.000
Cantidad de Interfaces Soportadas	2
Cantidad de Virtual CPU's (Mínimo)	2
Memoria Requerida (Mínimo)	4GB

3.1.2 Ítem C (Adquisición de un firewall de aplicaciones web (waf)):

Debido a que SOFSE tiene implementado en su infraestructura de ARSAT la solución de *F5 Network BIG-IP i2600 Advanced Web Application Firewall (appliance),* en la presente contratación se requiere una solución de la misma marca pero con mejores prestaciones que la mencionada para poder implementar ambas en alta disponibilidad, es decir, redundante a fallos. Como mínimo la solución ofertada debe ser la siguiente:

- F5 Network BIG-IP i4600 Advanced Web Application Firewall (appliance físico).
- F5 Networks F5-ADD-BIGI48XX
- F5 Networks F5-ADD-BIGI28XX

Deberá contar con las siguientes características de fuentes e interfaces:

- 8 SFP 1GB Cobre.

- SFP 1GB Fibra.
- 1 AC power suppliy adicional.

3.1.3 Ítem E (Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)):

Para el sistema SIEM solicitado se requieren las siguientes características mínimas:

(1) Número de dispositivos soportados/licenciados: 175.
(2) Número de agentes avanzados: 125.
(3) Implementación virtual.

Contexto en tiempo real para análisis de seguridad

(4) Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.
(5) Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad.
(6) Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización.
(7) Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados.

Biblioteca de remediación

(8) Disponibilidad de un conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.
(9) Posibilidad de ampliar esta biblioteca con desarrollo de scripts personalizados.

Informes de Cumplimiento Out-of-the-Box

(10) Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, como ser: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls.

Supervisión del rendimiento

(11) Monitor de métricas de sistema.
- Estado del sistema a través de SNMP, WMI, PowerShell.
- Estado de aplicaciones a través de JMX, WMI, PowerShell.
- Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster.

(12) Uso de almacenamiento, monitorización de rendimiento.

(13) Monitorización del rendimiento de aplicaciones a medida.
- Microsoft Active Directory y Exchange a través de WMI y Powershell.
- Bases de datos - Oracle, MS SQL, MySQL a través de JDBC.
- Infraestructura VoIP a través de IPSLA, SNMP, CDR / CMR.

(14) Posibilidad de agregar métricas personalizadas.
(15) Métricas de base y detección de desviaciones.

Supervisión del cambio de configuraciones en tiempo real

(16) Recopilar archivos de configuración de red, almacenados en un repositorio versionado.
(17) Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado.
(18) Detección automatizada de cambios en la configuración de la red y el software instalado.
(19) Detección automatizada de cambios de archivos y carpetas - Windows y Linux - quién y qué.
(20) Detección automatizada de cambios desde un archivo de configuración.
(21) Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente.

Contexto del dispositivo y de la aplicación

(22) Dispositivos de red incluyendo switches, routers, WLAN.
(23) Dispositivos de seguridad - Firewalls, IPS de red, gateways Web/Mail, protección contra malware, escáneres de vulnerabilidades.
(24) Servidores, incluyendo Windows, Linux.
(25) Servicios de infraestructura incluyendo DNS, DHCP, DFS, AAA, controladores de dominio, VoIP.
(26) Aplicaciones orientadas al usuario, incluidos servidores Web, servidores de aplicaciones, correo, bases datos.
(27) Dispositivos de almacenamiento como NetApp, EMC, Isilon, Nutanix, Data Domain.
(28) Dispositivos ambientales como UPS, HVAC, hardware del dispositivo.
(29) Infraestructura de virtualización incluyendo VMware ESX, Microsoft HyperVScalable.

Recolección de logs escalable y flexible

(30) Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores - tanto locales como en la nube.
(31) Los agentes de Windows proporcionarán una colección de eventos altamente escalable y rica, incluida la supervisión de integridad de archivos, los cambios de software instalados y la supervisión de cambios en el registro.
(32) Agentes de Linux para la supervisión de integridad de archivos.
(33) Capacidad de hash de ficheros vía File Integrity Monitoring utilizando SHA256.
(34) Protección de la integridad de los logs almacenados en la plataforma utilizando SHA256.
(35) Capacidad para modificar los analizadores directamente desde la interfaz gráfica de usuario y aplicarlos en el sistema en ejecución sin pérdida de tiempo de inactividad y de evento.
(36) Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación.
(37) Recopilación segura y fiable de eventos para usuarios y dispositivos ubicados en cualquier lugar.

Notificación y Gestión de Incidentes

(38) Framework de notificación de incidentes basado en políticas.
(39) Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico.
(40) Integración basada en API a sistemas externos de ticketing.
(41) Sistema incorporado de ticketing.

Paneles de control personalizados

(42) Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs.
(43) Informes y análisis exportables entre organizaciones y usuarios.
(44) Identificación rápida los problemas críticos, por ejemplo a través de un código de colores.
(45) Actualización rápida mediante el cálculo en memoria, sin acceso a disco.
(46) Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas.

Integración con fuentes de Inteligencia Externas

(47) API para integrar inteligencia externa de amenazas - dominios de malware, IPs, URL, hashes, nodos Tor, etc.
(48) Integración para fuentes de inteligencia de amenazas populares - ThreatStream, CyberArk, SANS, Zeus, etc.
(49) Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real.

Analítica detallada y escalable

(50) Búsqueda de eventos en real - sin necesidad de indexación.
(51) Búsquedas por palabras clave basadas en atributos de eventos analizados.
(52) Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
(53) Match de patrones complejos en tiempo real.
(54) Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas.
(55) Programación de informes y entregas de resultados por correo electrónico a los principales interesados.
(56) Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.).
(57) Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico.
(58) Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.

(59) Análisis escalable mediante la adición de nodos en caliente.
(60) Posibilidad de priorización de los informes de incidentes.

Detección de anomalías

(61) Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.
(62) Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base.
(63) Disparadores incorporados y personalizables sobre anomalías de comportamiento.

Integraciones de Tecnología Externa

(64) Integración con cualquier sitio web externo para la búsqueda de direcciones IP.
(65) Integración basada en API para fuentes externas de inteligencia de amenazas.
(66) Integración bidireccional basada en API con sistemas de help desk.
(67) Integración bidireccional basada en API con CMDB externas.
(68) Soporte de Kafka para la integración con informes mejorados de análisis, por ejemplo, ELK, Tableau y Hadoop.
(69) API para una fácil integración con sistemas de aprovisionamiento.
(70) API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.

Administración Simple y Flexible

(71) GUI basada en web, a ser posible HTML5.
(72) Control de acceso basada en roles para restringir el acceso a la GUI y a los datos.
(73) Todas las comunicaciones entre módulos están protegidas por HTTPS.
(74) Auditoría completa de la actividad del usuario.
(75) Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos.
(76) Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla.
(77) Archivado basado en políticas.
(78) Hashing de registros a tiempo para no repudio y verificación de integridad.
(79) Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta.

Capacidad de Escalamiento

(80) Escalabilidad de recolección de datos mediante la implementación de máquinas virtuales con la función de recolección (colectores virtuales).
(81) Los recolectores deben poder almacenar en búfer eventos cuando la conexión no esté disponible.
(82) Escalado del análisis mediante la implementación de nuevas máquinas virtuales.

(83) Arquitectura de balanceo integrada para recoger eventos desde sitios remotos usando recolectores.

Supervisión de disponibilidad

(84) Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
(85) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
(86) Monitorización del hardware y del entorno.
(87) Calendario para la programación de las ventanas de mantenimiento.
(88) Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.

Almacenamiento

(89) Posibilidad de implementar almacenamiento online vía ElasticSearch (ELK).
(90) Soporte de archivado de logs tanto para NFS como HDFS.
(91) Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.

3.2 Curriculums Vitae

El OFERENTE deberá de forma MANDATORIA especificar NOMBRE Y APELLIDO del equipo propuesto detallando sus respectivos Curriculums Vitae, para ser evaluado.

3.3 Especificaciones para la presentación y evaluación de las propuestas técnicas

A continuación, se detalla el ÍNDICE en que el OFERENTE debe presentar la documentación:

- Propuesta de servicios: Descripción de la propuesta de servicios, niveles de escalamiento, contactos y niveles de servicio.
- CV y Certificaciones: CV y Certificaciones que posee el personal que participará en el servicio. Ver Anexo 1, hoja 2.
- Referencias y proyectos de clientes: Listado de referencias y proyectos en clientes que tienen el servicio ofertado. Ver Anexo 1, hoja 1.

Todo documento que el OFERENTE considere que deba ser firmado por SOFSE luego de la adjudicación, deberá ser presentado conjuntamente con la oferta técnica. En tal sentido, se advierte que los citados documentos serán suscriptos con carácter exclusivo entre SOFSE 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).

SOFSE realizará una evaluación de las propuestas técnicas basándose en:

- Información del oferente requerida en los Pliegos
- Información de carácter público del OFERENTE

3.4 Admisión de las Ofertas

En aras de garantizar la adecuada comparación de Ofertas, de acuerdo a los principios rectores de la Contratación según el Reglamento de Compras y Contrataciones de SOFSE y el PBCG, el análisis de las propuestas presentadas se ajustará los lineamientos que se detallarán en los apartados siguientes:

Criterios mínimos de admisibilidad:

Las personas jurídicas interesadas deberán cumplir con los siguientes requisitos mínimos:

El personal afectado al PROYECTO deberá tener dominio del idioma español, al menos los miembros que tengan contacto con los usuarios y responsables de documentación, y presencia local permanente a partir de la fecha de inicio de tareas y hasta el cumplimiento del SERVICIO, o en las instancias que alcanzan a cada miembro del equipo afectado.

La oferta será considerada no admisible si no se cumple con las capacidades y antecedentes enunciados en Artículo 3°. CAPACIDADES DEL OFERENTE Y ESPECIFICACIONES DE PROPUESTAS.

Cumplir con los plazos y esfuerzos mínimos establecidos en la sección 2.3.1 Plazo de ejecución.

Evaluación de las Ofertas:

Regla General por Evaluación Económica:

Como regla general se adjudicará a la oferta de menor importe entre todas las presentadas.

3.5 Adjudicación

La adjudicación será POR LA TOTALIDAD DE LOS SEIS (6) ÍTEMS, de conformidad con las pautas establecidas en el presente documento y NO se aceptarán ofertas parciales.

3.6 Especificaciones para la presentación de propuestas económicas:

Las ofertas económicas 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.

SOFSE 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 OFERTA ECONOMICA será proporcionado sin costo alguno.

Las OFERTAS ECONOMICAS no podrán presentarse basadas en supuestos o consideraciones especiales ni sujetas a condición alguna.

TRENES ARGENTINOS OPERACIONES

Ministerio de Transporte
Presidencia de la Nación

Anexo 1: Perfil Organizacional y Equipo Propuesto

Hoja 1: Perfil Organizacional

Detalle de las Experiencias de Trabajo del Oferente

OFERENTE:

Año	Cliente / Proyecto	Rol / Servicio prestado	Tamaño del Proyecto	Industria	Alcance Funcional

Hoja 2: Equipo Nominado

Detalle de las Experiencias del Equipo de Trabajo del Oferente

OFERENTE:

Nombre y apellido del recurso propuesto	Rol Propuesto	Disciplina Tecnica	Area funcional / Frente	Años de experiencia en el rol propuesto	Experiencia en Proyecto: Empresa / Rol / Duración	Título Universitario y/o Carrera Postgrado	Certificaciones	Si eligio Certificaciones = "Otros", detallar	Herramientas	Experiencia en Herramientas

TRENES ARGENTINOS OPERACIONES

Ministerio de Transporte
Presidencia de la Nación

Anexo A: Planilla de Cotización

ANEXO A - PLANILLA COTIZACIÓN

Contratación N°:
Clase de Contratación:
Expediente:

Objeto: ADQUISICION DE BIENES Y SERVICIOS CONEXOS DE TECNOLOGIAS DE SEGURIDAD INFORMÁTICA

Adjudicación : Total

DETALLE PROVEEDOR	
Razón Social	
C.U.I.T.	

Renglón	Cantidad	U/M	Descripción	MONEDA	Precio Unitario	Subtotal
A	1	C/U	Adquisición de un firewall de nueva generación (ngfw)			0,00
B	24	C/U	Servicios de implementación y soporte del firewall de nueva generación (ngfw)			
C	1	C/U	Adquisición de un firewall de aplicaciones web (waf)			0,00
D	24	C/U	Servicios de implementación y soporte del firewall de aplicaciones web (waf)			
E	1	C/U	Adquisición de una solución de análisis y correlación de eventos de seguridad (siem)			
F	24	C/U	Servicios de implementación y soporte de la solución de análisis y correlación de eventos de seguridad (siem)			0,00
			Subtotal			**0,00**
			I.V.A.			**-**
			TOTAL			**0,00**

TRENES ARGENTINOS OPERACIONES

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Pliego Especificaciones Tecnicas

Número: IF-2022-55564609-APN-GSYP#SOFSE

CIUDAD DE BUENOS AIRES
Jueves 2 de Junio de 2022

Referencia: EX-2022-29582639- -APN-SG#SOFSE - Nuevo Pliego de Especificaciones Técnicas - “ADQUISICION DE BIENES Y SERVICIOS CONEXOS DE TECNOLOGIAS DE SEGURIDAD INFORMÁTICA”

El documento fue importado por el sistema GEDO con un total de 42 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.06.02 16:10:44 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2022.06.02 16:10:44 -03:00