ANEXO 6

Planilla de Verificación de Especificaciones Técnicas

ANDE	Dpto. de Tecnología Informática División de Tecnología y Desarrollo Informático Dirección de Telemática	Nº: 310325
	PLANILLA DE ESPECIFICACIONES TÉCNICAS y DATOS GARANTIZADOS	**Hoja: 1/11**
Referencia	*Actualización de Licencias, Soporte y mantenimiento para Equipo de Control de Amenazas Centralizadas (UTM SonicWall)*	

Objeto: Establecer las condiciones mínimas a ser cumplidas para la obtención de la actualización de licencias y soporte y mantenimiento preventivo y correctivo de los equipos de Control de Amenazas Centralizadas (UTM SONICWALL), bajo el fiel cumplimiento de lo establecido en la Planilla de Datos Garantizados que acompaña esta planilla de especificaciones técnicas.

De las especificaciones técnicas obligatorias: El proveedor deberá especificar concretamente en su propuesta para el objeto, servicios y soporte que atiendan obligatoriamente, las siguientes especificaciones técnicas. Además de completar la Planilla de Datos Garantizados que se provee.

Especificaciones Técnicas	Características	Mínimo Exigido	El Servicio Ofertado Cumple con las especificaciones requeridas (Si/No) SEKIURA
Situación actual	La institución cuenta con dos equipos Sonic Wall NSA los cuales operan en modalidad standalone conectados a proveedores de internet.	Exigido	
	La institución tiene implementado ambos equipos en modalidad HA y pretende la actualización de las licencias que poseen los equipos, además de un servicio de soporte y mantenimiento que mejore la performance para hacer frente a los nuevos ciberataques en tiempo real.		
ITEM 1 - ACTUALIZACIÓN DE LICENCIAS			
Provisión de licencias	Firewall SSL VPN para la solución HA	100	*CUMPLE
	Content Filtering	Exigido	*CUMPLE
	Capture Advanced Threat Protection	Exigido	*CUMPLE
	Gateway Anti-Virus / Anti- Spyware	Exigido	*CUMPLE
	Application Firewall Service and networking	Exigido	*CUMPLE
	Intrusion Prevention	Exigido	*CUMPLE
	App Control	Exigido	*CUMPLE
	Descifrado e inspección TLS/SSL/SSH	Exigido	*CUMPLE
	High Availability – heredando el secundario toda la configuración del primario	Exigido	*CUMPLE
	Tecnología SD-WAN para interconectar sedes remotas	Exigido	*CUMPLE
	VPN SSL 3000 (tres mil)	Exigido	*CUMPLE
	VPN IPSec	Exigido	*CUMPLE
	Sistema de filtrado de navegación Web	Exigido	*CUMPLE
	Protección anti DoS	Exigido	*CUMPLE
	Analytics Software	Exigido	*CUMPLE
	Cantidad de Licencias para HA	Exigido	*CUMPLE
	Cantidad de Usuarios 3000 (tres mil)	Exigido	*CUMPLE
	Actualizaciones por 3 años	Exigido	*CUMPLE
	Los derechos de las suscripciones/licencias deberán estar a favor de la ANDE utilizando su respectiva cuenta.	Exigido	*CUMPLE
ITEM 2 - SOPORTE Y MANTENIMIENTO			
Servicio de Actualización	SONICWALL COMPREHENSIVE GATEWAY SECURITY SUITE-W VIEWPOINT	Exigido	*CUMPLE
	SonicWALL Advanced Gateway Security Suite para la solución HA		

Soporte y Garantía	Se deberá ofrecer el servicio de soporte técnico local por parte del oferente con técnicos certificados por el fabricante por 36 meses en la sgte modalidad: **1. Mecanismo para solicitar el soporte** • Portal de Servicios en Línea: Sistema de tickets disponible en [URL del portal]. • Correo Electrónico: Envío de incidencias vía correo electrónico. • Teléfono de Soporte: Llamada directa al número para incidencias de severidad Crítica (Nivel 1). • Cada ticket tendrá un **ID único** y trazabilidad de atención. **2. Niveles de severidad y tiempos de respuesta** El tiempo de respuesta se define como el plazo máximo entre la recepción de la incidencia por parte del Proveedor y la primera respuesta formal por parte del equipo de soporte del mismo. **Nivel 1: Crítico** • **Impacto:** Interrupción total o grave del servicio de red. Caída completa del firewall, pérdida de conectividad crítica, denegación de servicio generalizada. **Ejemplo:** El dispositivo no responde; toda la conectividad de Internet/WAN está caída. • **Tiempo de Respuesta (TR): ≤ 1 horas** • **MTTR (resolución completa): ≤ 4 horas** **Nivel 2: Alto** • **Impacto:** Degradación severa del servicio o interrupción parcial que afecta a un grupo significativo de usuarios o servicios críticos. **Ejemplo:** Caída de una VPN Site-to-Site crítica, pérdida de funcionalidad clave como el filtrado de malware. • **Tiempo de Respuesta (TR): ≤ 2 horas** • **MTTR (resolución completa): ≤ 8 horas** **Nivel 3: Medio** • **Impacto:** Problema no crítico con impacto moderado en el servicio. Funcionalidad reducida pero no interrumpida. **Ejemplo:** Problemas intermitentes de rendimiento, alertas específicas no críticas en los logs. • **Tiempo de Respuesta (TR): ≤ 6 horas** • **MTTR (resolución completa): ≤ 72 horas hábiles** **Nivel 4: Bajo** • **Impacto:** Consultas, solicitudes de información o problemas menores sin impacto perceptible en el servicio operativo. **Ejemplo**: Consultas sobre configuración, solicitud de documentación. • **Tiempo de Respuesta (TR): ≤ 8 horas** • **MTTR (resolución completa): ≤ 72 horas hábiles** **TR** mide **cuán rápido responde** el proveedor al aviso. **MTTR** mide **cuán rápido soluciona** efectivamente el problema. **3. Compromisos / Tareas del proveedor** **Compromisos del Proveedor:** • Cumplir con los tiempos de respuesta definidos para cada nivel de severidad. • Realizar un diagnóstico remoto del problema. • Brindar soluciones de trabajo (workarounds) o parches temporales mientras se encuentra una resolución permanente. • Gestionar la escalación del caso con el soporte técnico de SonicWall (TAC) cuando sea necesario. • Mantener una comunicación clara y proactiva con la convocante durante el proceso de resolución.	Exigido	*CUMPLE

- Incluir dentro del servicio de soporte la actualización periódica de firmware a la última versión liberada por el fabricante, especialmente aquellas asociadas a seguridad y estabilidad del sistema.
- Reemplazar sin costo adicional todas las partes dañadas por desperfectos de fabricación o desgaste de uso, asegurando que las partes nuevas sean originales y provistas por el fabricante. Si los equipos están descontinuados por el fabricante, de manera que ello impida la provisión de soporte, el recambio de partes, la actualización de firmware o la activación de alguno de los servicios descritos en estas especificaciones técnicas, el proveedor deberá sustituirlos por equipos iguales o de mayores prestaciones, sin costo adicional para la Contratante, a fin de mantener la cobertura de soporte por parte del fabricante. En caso de reemplazo, los nuevos equipos deberán ser instalados y configurados por técnicos del proveedor certificados por el fabricante.

Tareas del Proveedor:

- Monitorizar la canalización de incidencias.
- Asignar recursos técnicos adecuados al nivel de severidad.
- Realizar seguimiento activo y documentado de los casos abiertos hasta su resolución definitiva.
- Proveer reportes mensuales de cumplimiento del SLA, incluyendo indicadores de disponibilidad, tiempos de respuesta, MTTR, reposiciones realizadas y tickets atendidos.
- Brindar entrenamiento inicial al personal designado por la Contratante, con un mínimo de 40 horas de capacitación dirigidas a al menos 4 funcionarios, así como capacitaciones de actualización cuando se implementen cambios relevantes en la solución. El proveedor deberá entregar materiales de apoyo y certificados de participación al finalizar las capacitaciones.

4. Indicadores y Metas Mínimas (KPI)

Indicador (KPI)	Definición	Meta Mínima
Disponibilidad del Servicio	(Tiempo Total - Inactividad) / Tiempo Total * 100	**≥ 99.5% mensual**
Tiempo Medio de Respuesta (TR)	Tiempo promedio desde la recepción del ticket hasta el primer contacto técnico.	Cumplimiento ≥95 % de los objetivos del punto 2 (Niveles de severidad y tiempos de respuesta).
MTTR crítico	Tiempo promedio desde la recepción del ticket hasta la resolución completa del incidente Nivel 1 (Crítico).	≤ 4 horas
Resolución en primera atención (incidencias de niveles 2–4)	Porcentaje de tickets atendidos dentro de los tiempos de respuesta acordados	≥ 95 %
Reposición de hardware	Tiempo para reemplazar equipos tras reclamo	≤ 72 horas hábiles

5. Mecanismos de control y supervisión

- **Sistema de Ticketing:** Todas las incidencias serán gestionadas a través de un sistema de ticketing. El Cliente tendrá acceso a un portal para ver el estado de sus tickets.
- **Informes Mensuales de Cumplimiento:** El Proveedor entregará al Cliente, durante la primera semana de cada mes, un informe detallado que incluirá:
  - Resumen de todos los tickets del mes con ID, severidad, apertura/cierre.
  - Cumplimiento de los tiempos de respuesta (TR) y resolución (MTTR) por severidad.
  - Cálculo de la disponibilidad de cada dispositivo.
  - Reposiciones realizadas.

JM.

	○ Análisis de causas raíz para incidencias recurrentes o críticas. **6. Penalizaciones por incumplimiento** Las penalizaciones aplicables durante la vigencia del contrato por incumplimiento de los niveles de servicio (SLA) serán independientes de la multa prevista en la sección CONDICIONES CONTRACTUALES - Porcentaje de multas del Pliego, la cual corresponde exclusivamente a los atrasos en el inicio de la prestación del servicio. En caso de que el Proveedor no cumpla con las metas mínimas establecidas en los KPI del punto 4, se aplicará el siguiente esquema de multas, los cuales se descontarán de la factura mensual siguiente al incumplimiento: • **Disponibilidad del servicio:** cuando la disponibilidad mensual sea inferior al 99,5 %, se aplicará una penalización equivalente al 0,5 % del monto mensual del servicio por cada 1 % de déficit. • **Tiempo de respuesta a incidentes:** si el tiempo de respuesta (TR) excede los valores máximos establecidos en el punto 2 (Niveles de severidad y tiempos de respuesta), se aplicará una penalización equivalente al 0,2 % del monto mensual del servicio por cada hora que exceda los tiempos máximos establecidos. • **Tiempo Medio de Restauración (MTTR) en incidentes críticos:** cuando la resolución exceda las 4 horas, se aplicará una penalización del 1 % del monto mensual del servicio por cada 4 horas adicionales de atraso. • **Reposición de hardware:** en los casos en que la reposición de equipos supere las 72 horas hábiles desde la notificación escrita de la Contratante, se aplicará una penalización adicional del 1 % del monto mensual del servicio por cada día hábil adicional de atraso. Esta penalización aplica exclusivamente a reposiciones derivadas de fallas o descontinuación del fabricante durante la vigencia del contrato, conforme lo señalado en los compromisos del proveedor. • **Resolución en primera atención (niveles 2–4):** cuando el porcentaje de tickets de severidad media o baja resueltos en primera atención sea inferior al 95 % mensual, se aplicará una penalización equivalente al 0,2% del monto mensual del servicio por cada 1% de déficit. Las penalizaciones establecidas no liberan al proveedor del cumplimiento de sus obligaciones contractuales y serán deducidas de la factura correspondiente al mes siguiente al incumplimiento. El monto total de las penalizaciones aplicadas en un mes no podrá superar el diez por ciento (10 %) del monto mensual del servicio. **Nota:** Quedan excluidas de este régimen de penalizaciones las incidencias causadas por fuerza mayor, actuación del Cliente o de terceros no autorizados por el Proveedor, o falta de acceso remoto proporcionado por la convocante.		
Certificación del Fabricante	El proveedor deberá presentar la Autorización del fabricante dirigida a la convocante especificando el número de ID de la licitación, para proveer el software y brindar soporte específico para la presente licitación. La empresa oferente deberá contar con las certificaciones: ISO 9001: "Sistema de Gestión de Calidad" e ISO 27001: "Sistema de Gestión de Seguridad de la Información" o equivalentes. La exigencia de la certificación ISO 9001 o similar tiene por finalidad asegurar que el proveedor cuente con procesos organizacionales formales, controlados y orientados a la mejora continua. La provisión de servicios asociados a infraestructura crítica de red, como lo es la plataforma de seguridad UTM actualmente en uso, requiere que los proveedores cumplan estándares de calidad que aseguren la entrega sistemática y eficaz de servicios, así como la trazabilidad de sus procesos. Esta certificación también actúa como un parámetro objetivo y verificable de madurez organizacional.	Exigido	**CUMPLE

	La certificación ISO 27001 o similar responde a la naturaleza crítica de la información que será procesada, protegida y monitoreada por la solución. Esta norma internacional garantiza que la empresa cuente con un sistema de gestión integral para proteger la confidencialidad, integridad y disponibilidad de la información, lo cual es indispensable tratándose de una solución de ciberseguridad que, entre otros aspectos, administra conexiones VPN, reglas de firewall, prevención de intrusiones y control de aplicaciones. Además, al exigir esta norma, se busca que el proveedor adopte políticas claras de seguridad, que protejan tanto a la convocante como a terceros frente a posibles incidentes, brechas o malas prácticas.		
Técnicos Certificados	El oferente deberá presentar con la oferta: El proveedor local deberá contar con al menos 1 (un) técnico certificado en la marca ofertada, para garantizar el buen servicio y respaldo del soporte local. Deberá contar con al menos 1 (un) técnico con la certificación CEH o equivalente, para garantizar la seguridad en las configuraciones e implementación del equipo solicitado. La exigencia de contar con al menos un técnico certificado por el fabricante SonicWall y otro con formación en ciberseguridad (CEH o equivalente) responde a una necesidad técnica directa e ineludible. El soporte local requerido debe ser altamente especializado y debería contemplar tareas como: Activación y configuración de funciones avanzadas (IPS, DPI-SSL, control de aplicaciones, Content Filtering, etc.). Diagnóstico y resolución de incidencias críticas. Aplicación de políticas de seguridad a nivel de red corporativa. Estas tareas exigen que el personal técnico tenga dominio específico del producto y de buenas prácticas de ciberseguridad internacionalmente reconocidas. La certificación CEH (Certified Ethical Hacker) garantiza que el técnico maneje técnicas avanzadas en hacking ético para así poder entender cómo operan los atacantes y cómo proteger efectivamente la infraestructura contra amenazas complejas. Los técnicos propuestos deben presentar certificaciones vigentes relacionadas soluciones dedicadas a la ciberseguridad a la fecha de presentación de la oferta, que avalen la formación y experiencia Los técnicos deben formar parte del plantel de la empresa oferente, con al menos 1 (un) año de antigüedad, comprobable con la planilla de inscripción en IPS. Este requerimiento tiene por objetivo garantizar continuidad, responsabilidad y trazabilidad del servicio prestado, y evitar prácticas como la subcontratación eventual de personal sin experiencia con el entorno de la convocante.	Exigido	*CUMPLE
Activación y configuración de Content Filtering	Control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 56 categorías y deberán actualizarse automáticamente.	Exigido	*CUMPLE
	Soporte a Youtube en modo restringido	Exigido	*CUMPLE
	Ser capaz de forzar el uso del safe search en google y bing	Exigido	*CUMPLE
	Evitar el uso de URLs embebidas (por ejemplo Google Translate) para evadir el filtrado web	Exigido	*CUMPLE
	Soportar mecanismos de Autenticación: RADIUS, TACACS+, Active Directory, LDAP, base de datos interna, Reconocimiento transparente de usuario del LDAP, reconocimiento de usuarios presentes en Terminal services (Windows y Citrix) y usuarios locales	Exigido	*CUMPLE
	Reconocimiento transparente (sin validación adicional) de los usuarios ya autenticados a través de un RADIUS server usando información de RADIUS accounting	Exigido	*CUMPLE

	Definición de cuota diaria, semanal o mensual de tiempo de conexión o de tráfico generado por cada usuario	Exigido	*CUMPLE
	Filtrado de páginas web sobre usuarios que no estén dentro de la red a través de un cliente de filtrado web	Exigido	*CUMPLE
Activación y configuración de Capture Advanced Threat Protection	Servicio online de detección de virus en la nube con capacidad de reconocimiento de más de 70 millones de amenazas el cual se puedan enviar muestras resumidas del tráfico para detectar códigos maliciosos	Exigido	*CUMPLE
	Filtrado de conexiones a centros de control de Botnets basado en reputación de direcciones IP	Exigido	*CUMPLE
	Controles de localización geográfica basados en la dirección IP de origen para hacer reglas de conexión por país bien sea de manera general o por reglas de firewall	Exigido	*CUMPLE
Activación y configuración de Gateway Anti-Virus Anti-Spyware	Rendimiento de Gateway Antivirus de 5 Gbps usando el modo de operación (Proxy o Flow) que brinda la máxima seguridad.	Exigido	*CUMPLE
	Analizar, tráfico entrante y saliente mínimo de los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, CIFS/NETBIOS, y esta debe estar completamente integrada a la administración del dispositivo appliance	Exigido	*CUMPLE
	Escaneo de virus o spyware sobre protocolos basados en stream TCP, como Mensajería Instantánea y P2P	Exigido	*CUMPLE
	Análisis antivirus sin limitación del tamaño del archivo transferido y sin que esto afecte la efectividad de la detección de amenazas	Exigido	*CUMPLE
	El sistema antivirus deberá contar con la certificación Antivirus ICSA labs	Exigido	*CUMPLE
	Actualizaciones automáticas con un intervalo mínimo de búsqueda de actualizaciones de 1 hora	Exigido	*CUMPLE
Mejora de perfomance y configuración de Application Firewall Service and networking	La Cantidad Mínima de sub-interfaces VLANs será de 500	Exigido	*CUMPLE
	Enrutamiento basado en políticas para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, la direcciones IP de origen o de destino	Exigido	*CUMPLE
	Enrutamiento basado en la aplicación, por ejemplo, Office 365 se encaminan por una interface de salida a internet mientras que YouTube se encamina por otra	Exigido	*CUMPLE
	Enrutamiento basado en políticas basado en el Full Qualified Domain Name – FQDN	Exigido	*CUMPLE
	Equal Cost Multipath para balanceo de rutas a través de múltiples canales	Exigido	*CUMPLE

	Tecnología SD-WAN para interconectar sedes remotas usando enlaces de internet de bajo costo pero con alta calidad de conexión	Exigido	*CUMPLE
	Enrutamiento: BGP, OSPF, RIPv1/v2, rutas estáticas y Multicast	Exigido	*CUMPLE
	Link aggregation tanto estático como dinámico	Exigido	*CUMPLE
	Redundancia de puertos	Exigido	*CUMPLE
	Capacidad de realizar backups de la configuración automáticamente también respaldarlos en la nube	Exigido	*CUMPLE
	Port Mirroring	Exigido	*CUMPLE
	(QoS) Garantizar comunicaciones críticas con 802.1p, etiquetado DSCP y reasignación de tráfico VoIP en la red.	Exigido	*CUMPLE
	Protección contra ataques DoS	Exigido	*CUMPLE
	Balanceo de carga de múltiples interfaces WAN utilizando los métodos Round Robin, Spillover o Percentage.	Exigido	*CUMPLE
	El Rendimiento mínimo de Firewall de 17 Gbps usando la metodología de medición basada en el RFC 2544.	Exigido	*CUMPLE
	La cantidad mínima de conexiones que el sistema deberá soportar en modo firewall será de al menos 10 Millones	Exigido	*CUMPLE
	Soportar 130 mil conexiones por segundo	Exigido	*CUMPLE
	Cantidad mínima de conexiones del sistema con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI) será de 4 millones	Exigido	*CUMPLE
	Certificación ICSSA Labs para Firewall	Exigido	*CUMPLE
	Certificación Common Criteria NDPP, Firewall e IPS	Exigido	*CUMPLE
	Certificación FIPS 140-2	Exigido	*CUMPLE
	Deberá soportar DNS Sinkhole	Exigido	*CUMPLE
	Deberá soportar DNS Tunnel Detection	Exigido	*CUMPLE
Activación y configuración de Intrusion Prevention System	Rendimiento mínimo en IPS : 10 Gbps	Exigido	*CUMPLE
	El sistema IPS contará con al menos 4.800 firmas de ataques	Exigido	*CUMPLE
	Protección de ataques de inundación (flood) a nivel de UDP, ICMP y el conocido SYN Flood	Exigido	*CUMPLE
	Permitir al administrador ejecutar acciones sobre los eventos de IPS como bloquear el tráfico, registrar o capturar el tráfico generado por el ataque	Exigido	*CUMPLE
	El IPS podrá inspeccionar el tráfico entre las zonas internas de la red	Exigido	*CUMPLE
	Deberá contar con mecanismos de antievasión	Exigido	*CUMPLE

	Filtro de bloqueo hacia centros de comando y control de botnets	Exigido	*CUMPLE
	Filtro de bloqueo por localización geográfica granular por cada regla de firewall	Exigido	*CUMPLE
Activación y Configuración de App Control	El rendimiento mínimo del sistema de control de aplicaciones será de 11 Gbps	Exigido	*CUMPLE
	identificar, categorizar y controlar y visualizar tráfico de más de 4300 aplicaciones agrupadas en al menos 25 Categorías	Exigido	*CUMPLE
	Las aplicaciones se deben identificar independientemente del Stack o del puerto (TCP, UDP, etc.) que usen	Exigido	*CUMPLE
	Las políticas de control de aplicaciones se podrán hacer granular por dirección IP, usuario, grupos de usuarios locales o de LDAP/Active Directory y basado en horarios.	Exigido	*CUMPLE
	Creación de reglas de control de ancho de banda de las aplicaciones soportadas	Exigido	*CUMPLE
	Reportar en tiempo real cuales de las aplicaciones soportadas están siendo usadas, que usuario o dirección IP lo está haciendo y cuánto tráfico está cursando	Exigido	*CUMPLE
Activación y configuración de Descifrado e inspección DPI-SSL/TLS/SSH	Inspección de Aplicaciones, IPS, antivirus y filtrado de páginas web sobre comunicaciones cifradas por TLS (Transport Layer Security) tales como HTTPS sin importar si opera sobre el puerto 443 u otro	Exigido	*CUMPLE
	El sistema de inspección profunda de paquetes deberá funcionar bidireccionalmente	Exigido	*CUMPLE
	El sistema de inspección profunda de paquetes deberá operar sin proxies para evitar problemas de latencia	Exigido	*CUMPLE
	El Rendimiento en Inspección SSL será mínimo de 2 Gbps	Exigido	*CUMPLE
	Manejar como mínimo 500000 conexiones concurrentes de tráfico cifrado usando los módulos de protección (IPS, Antimalware y control de aplicaciones)	Exigido	*CUMPLE
	Inspección de tráfico cifrado sobre SSH	Exigido	*CUMPLE
	Se podrán definir excepciones al tráfico cifrado por dominios o por categorías de páginas web	Exigido	*CUMPLE
	Soportar conexiones DPI SSL hasta 200 mil	Exigido	*CUMPLE
High Availability	Alta Disponibilidad (HA) entre 2 equipos - heredando el secundario toda la configuración del primero	Exigido	*CUMPLE
Upgrade de Licencias VPN SSL	La cantidad mínima de túneles VPN Site to Site soportados será 12.000	Exigido	*CUMPLE
	El Mínimo Rendimiento de VPNs 3DES/AES será de 10 Gbps usando la metodología de medición basada en el RFC 2544.	Exigido	*CUMPLE
	El sistema contará con mínimo 3000 Licencias de cliente VPN para acceso remoto	Exigido	*CUMPLE
	El sistema permitirá autenticación biométrica para las conexiones VPN	Exigido	*CUMPLE
Analytics Software	Deberá tener Capture Security Center	Exigido	*CUMPLE

	Capture Security Center: Proporcionar un agente de informes de flujos para el análisis del tráfico de las aplicaciones y datos sobre el uso mediante protocolos IPFIX o NetFlow para ofrecer una supervisión en tiempo real e histórica. Ofrecer a los administradores una interfaz para supervisar visualmente su red en tiempo real. Identificar aplicaciones y páginas web con gran demanda de ancho de banda, visualizar el uso de las aplicaciones por usuarios y anticiparse a ataques y amenazas en la red.	Exigido	*CUMPLE
	• Visor en tiempo real personalizable mediante funciones de arrastrar y soltar.		
	• Pantalla de informes en tiempo real con filtrado de un solo clic.		
	• Dashboard de los flujos principales con botones de "Visualizar por" de un solo clic.		
	•Pantalla de informes de flujos con cinco pestañas de atributos de flujos adicionales.		
	• Pantalla de análisis de flujos con potentes funciones de correlación y dinamización.		
	•Visor de sesiones para el desglose profundo de sesiones individuales y paquetes.		
	Análisis del tráfico de aplicaciones, visión del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, prestaciones de análisis forenses y resolución de problemas.		

* Se verifica con documentación presentada según solicitado mediante SPD 01
** Se verifica con documentación solicitada SPD 03 Y SPD 01

Se realizó la verificación de documentación solicitada en SPD 01 y SPD 03, a oferente SEKIURA S.A.C.E.I, verificándose la siguiente documentación:

1. Las planillas de Datos Garantizados incluidas en las Especificaciones Técnicas, debidamente llenadas y firmadas, con los datos técnicos y valores en ellas solicitadas, se verifican las referencias a la documentación y se corroboran los datos según los catálogos presentados.

2. Fotocopia de los documentos de Certificaciones ISO 9001 vigente, con fecha de vencimiento 19/02/2027. Sistema de Gestión de Calidad e ISO 27001 vigente, con fecha de vencimiento 19/02/2027

3. Fotocopia de los documentos que avalen a los Técnicos Certificados de la marca ofertada y vigente relacionadas a soluciones dedicadas a la ciberseguridad. Certificación presentada del Señor Hector Perez, con certificado de SonicWall Technical Master, fecha junio 15 del 2022. Certificación presentada del Señor Cesar Verón, con certificado de SonicWall Technical Master, fecha junio 15 del 2021

4. Fotocopia de los documentos que avalen a los Técnicos Certificados con la certificación CEH o similar equivalente y vigentes relacionadas a configuraciones e implementación de equipos. Certificación presentada del Señor Nicolas Sato, CEH vigente, válido hasta 01 de abril del 2027. Certificación presentada del Señor Cesar Verón, CEHPC vigente, valido hasta 13 de diciembre del 2027.

5. Fotocopia de los documentos que forman parte del plantel de la Empresa Oferente y comprobable con la presentación de la planilla de inscripción en el Instituto de Previsión Social (IPS).
   Nicolas Sato, nro transacción: 84496154
   Hector Perez, nro transacción:14896903
   Cesar Verón, nro transacción:65016032

Se solicitó presentación de documentos para evaluación de capacidad técnica a oferente ITCS S.A. mediante SPD 02, no teniendo respuesta a lo solicitado.

Lic. Hugo Mujica
Oficina de Ciberseguridad