Necesidad por Atender

La Superintendencia requiere garantizar la continuidad operativa, disponibilidad y seguridad de las aplicaciones web institucionales que soportan sus procesos misionales y de atención a los ciudadanos. Actualmente, el dispositivo WAF FortiWEB 400E, en modalidad on-premise, cumple un rol crítico en la protección contra ataques cibernéticos tales como inyección de código, robo de credenciales, malware avanzado, ataques de denegación de servicio y otras amenazas dirigidas a la capa de aplicaciones.

El licenciamiento y soporte vigente del WAF on-premise finaliza el 23 de noviembre de 2025, por lo cual resulta indispensable renovar oportunamente las suscripciones y el soporte especializado con el fabricante, a fin de evitar la degradación o interrupción de los servicios de seguridad y mitigar riesgos de indisponibilidad, pérdida de información sensible y afectaciones a la infraestructura tecnológica institucional.

Adicionalmente, la entidad requiere fortalecer sus capacidades de protección en entornos de nube, mediante la adquisición de una suscripción de Web Application Firewall (WAF) que complemente y amplíe la cobertura de la solución actual on-premise, permitiendo la protección de los sistemas de información y portales web desplegados en Azure y otros entornos virtualizados. El crecimiento en la exposición de servicios en línea y la mayor demanda de accesibilidad por parte de los ciudadanos hacen indispensable contar con una solución en la nube que garantice alta disponibilidad, escalabilidad y continuidad operativa, protegiendo integralmente los portales web institucionales sin importar la infraestructura tecnológica utilizada.

De no contar con la renovación y la adquisición complementaria en la nube, la Superintendencia quedaría expuesta a vulnerabilidades críticas, interrupciones en la prestación de servicios digitales, pérdida de confianza ciudadana, posibles sanciones regulatorias por incumplimiento de estándares de seguridad de la información y una disminución en la capacidad de respuesta frente a incidentes de ciberseguridad.

En consecuencia, se hace necesario adelantar el proceso contractual que contemple tanto la renovación del soporte y licenciamiento del WAF FortiWEB 400E on-premise, como la adquisición e implementación de una suscripción de WAF en la nube, junto con los servicios de mantenimiento, monitoreo, soporte especializado y transferencia de conocimiento. Lo anterior permitirá a la Superintendencia fortalecer su esquema de seguridad perimetral, proteger de manera integral sus aplicaciones web y garantizar la continuidad, resiliencia y confianza en los servicios tecnológicos ofrecidos a la ciudadanía.

1. **CARACTERÍSTICAS TÉCNICAS DE LOS PRODUCTOS, BIENES, OBRAS O SERVICIOS PARA ON PREMISE:**

- Renovar, por el término de un (1) año a partir del 23 de noviembre de 2025, el soporte nivel Advance HW del dispositivo WAF FortiWEB 400E con el fabricante y las características funcionales: Firmware & General Updates, Enhanced Support, Telephone Support, Advance Malware Protecction, FortiWeb Security Service, IP Reputation, Credential Stuffing Defense, FortiSandbox Cloud y Threat Analitycs Service.
- Garantizar que el licenciamiento y soporte a adquirir inicie a partir de la fecha de

finalización del licenciamiento actual.

- Brindar asistencia técnica y gestión de requerimientos en modalidad 24x7 a partir del 23 de noviembre de 2025 y durante la vigencia del soporte del dispositivo.
- Realizar el monitoreo de salubridad y disponibilidad 7x24, el análisis de eventos y reportes de seguridad enviados por la plataforma durante la vigencia del soporte del dispositivo, por lo que deberá reportar al supervisor de manera inmediata, cualquier evento o ataque de seguridad identificado a través de los canales de comunicación que se establezcan al inicio del servicio; generar informes de funcionamiento y alertas, cumpliendo con los niveles de servicio definidos y asegurando la identificación temprana de amenazas o comportamientos anómalos
- Poner a disposición de la entidad las correcciones a posibles defectos que puedan existir en todos los componentes y/o herramientas que posee la plataforma durante la vigencia del soporte.
- Entregar un informe o reporte mensual del estado, comportamiento y funcionamiento del dispositivo correspondiente al periodo inmediatamente anterior durante la vigencia del soporte.
- Realizar dos (2) mantenimientos preventivos al dispositivo WAF durante la vigencia del soporte y presentar un informe del estado con el cual se encontró antes del mantenimiento y el estado posterior a la realización del mismo, en donde se indique la actualización del sistema operacional al más reciente, estable y recomendado por el fabricante, revisión y ajuste de configuración de acuerdo a las mejores prácticas (CIS y NIST SP 800-53), revisión del desempeño y las recomendaciones que sean necesarias. Se deberán realizar periódicamente los análisis del equipo y sus configuraciones para verificar el cumplimiento de mejores prácticas según el fabricante Fortinet.
- Realizar un plan de trabajo y/o cronograma de actividades, concertado con el supervisor, en un término no mayor a cinco (5) días hábiles posteriores a la firma del acta de inicio.
- Proponer y ejecutar acciones de mejora, ajustando configuraciones y reglas del WAF conforme a estándares y buenas prácticas de seguridad, para fortalecer la protección de las aplicaciones web institucionales.
- Entregar los materiales de apoyo y evidencias de la capacitación realizada, incluyendo presentaciones, manuales, guías de usuario, listas de asistencia firmadas y encuestas de satisfacción, los cuales deberán ser entregados en medio físico y/o digital, según lo defina la supervisión, como soporte de la ejecución del servicio.
- Realizar cinco (5) sesiones de transferencia de conocimiento al equipo de la superintendencia de la siguiente manera:
    - Dos (2) transferencias técnicas al personal designado por la superintendencia con una duración de mínimo de tres (3) horas cada una las cuales deberán ser dictadas por fuera de las instalaciones de la Superintendencia con un máximo de 15 personas de asistentes por sesión.
    - Tres (3) charlas de una (1) hora cada una, dirigidas al personal general de la superintendencia, las cuales, deberán tener como finalidad concientizar a los

asistentes acerca de la ciberseguridad. Estas charlas se realizarán de forma virtual previa aprobación del contenido de las cada una de ellas.

Las charlas se deberán programar para brindarse durante la prestación del servicio y estas deben estar plasmadas en el plan de trabajo que se debe presentar al inicio de la ejecución del contrato.

2. CARACTERÍSTICAS TÉCNICAS DE LOS PRODUCTOS, BIENES, OBRAS O SERVICIOS PARA NUBE:

- Entregar una suscripción para herramienta WAF (Web Application Firewall) del fabricante Fortinet, para ser implementada en nube (Azure) a partir del día diez (10) hábil de firmada el acta de inicio y vigente hasta el 22 de noviembre de 2026.
- La herramienta debe incluir: acceso a actualizaciones y parches liberados por el fabricante, disponibilidad del portal de soporte técnico con documentación, guías y recursos especializados, así como asistencia directa por parte del fabricante y el proveedor a través de canales habilitados como web, chat y línea telefónica.
- Debe admitir al menos 500 Mbps de tráfico HTTP, comprobado con documentación pública disponible en el sitio web del fabricante; por lo cual no se aceptarán cartas de fabricante para cumplir con este item.
- No debe tener limitación de aplicaciones protegidas; El Numero de Aplicaciones a proteger no deberá estar limitado por licenciamiento.
- Debe ser soportada por máximo cuatro (4) Core Virtuales.
- Debe ser soportada por máximo 16 GB de RAM Virtual.
- Debe ser soportada por máximo 2TB de almacenamiento
- Debe soportar alta disponibilidad
- Debe soporta mínimo 10 interfaces de red.
- Debe soportar los siguientes hipervisores VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, y Oracle Cloud. El licenciamiento debe poderse migrar a otras nubes o ambientes virtualizados para su uso como BYOL (Bring your own license)
- La herramienta de WAF ofertada debe ser 100% compatible con la que tiene la Entidad en On- Premise (Fortiweb 400E) para unificar administración, políticas y funcionalidades.
- El licenciamiento debe incluir como mínimo: Seguridad WEB con OWASP top 10, firmas WAF, reglas personalizadas, reputación IP, Antimalware, Sandbox cloud, Defensa de hurto de credenciales, analítica de riesgos, entre otras.
- Realizar la entrega de la suscripción de la herramienta a nombre de la Superintendencia del Subsidio Familiar.
- Realizar el monitoreo de salubridad y disponibilidad 7x24, el análisis de eventos y reportes de seguridad enviados por la plataforma durante la vigencia del soporte de la suscripción, por lo que deberá reportar al supervisor de manera inmediata, cualquier evento o ataque de seguridad a través de los canales de comunicación que se establezcan al inicio del contrato.

- Poner a disposición de la entidad las correcciones a posibles defectos que puedan existir en todos los componentes y/o herramientas que posee la plataforma durante la vigencia del soporte.
- Se deberán realizar periódicamente los análisis de la herramienta y sus configuraciones para verificar el cumplimiento de mejores prácticas según el fabricante Fortinet.
- Documentar detalladamente, toda la instalación, arquitectura y configuración de solución implementada en un documento que debe ser entregado a la entidad al finalizar la puesta en funcionamiento de la solución.
- La solución debe permitir fácil y rápidamente implementar controles basado en políticas internas hacia los servidores web de la entidad.
- La herramienta debe poder restaurar los portales web de forma automática en caso de presentarse una modificación no autorizada.
- La plataforma propuesta debe identificar vulnerabilidades a un número ilimitado de aplicativos webs de la entidad, sin requerir licenciamiento adicional.
- La herramienta debe contar con sus respectivas actualizaciones periódicas a nivel de firmas de seguridad durante el periodo contratado.
- La herramienta debe poseer la capacidad de ser implementada en modo Reverse Proxy.
- La herramienta debe contar con funcionalidades de Machine Learning.
- Realizar un plan de trabajo y/o cronograma de actividades, concertado con el supervisor, en un término no mayor a cinco (5) días hábiles posteriores a la firma del acta de inicio.
- Realizar dos (2) transferencias de conocimientos acerca del uso y configuración de la herramienta con una duración de tres (3) horas como mínimo para afianzar en conocimiento y experticia en seguridad de la información.
- Debe contar con un sistema de gestión formal que contemple buenas prácticas internacionales orientadas a la seguridad de la información en entornos de servicios en la nube, aplicado a los procesos relacionados con seguridad.
- Entregar los materiales de apoyo y evidencias de la capacitación realizada, incluyendo presentaciones, manuales, guías de usuario, listas de asistencia firmadas y encuestas de satisfacción, los cuales deberán ser entregados en medio físico y/o digital, según lo defina la supervisión, como soporte de la ejecución del servicio.
- Brindar cinco (5) sesiones de transferencia de conocimiento al equipo de la superintendencia de la siguiente manera:
    - Dos (2) transferencias técnicas para el personal designado por la superintendencia con una duración de mínimo de tres (3) horas cada una las cuales deberán ser dictadas por fuera de las instalaciones de la Superintendencia con un máximo de 15 personas de asistentes por sesión
    - Tres (3) charlas de una (1) hora cada una, dirigidas al personal de la superintendencia las cuales deberán tener como finalidad concientizar a los asistentes a estas sesiones, estas charlas se realizarán de forma virtual previa aprobación del contenido de las cada una de ellas.
    - Las charlas se deberán programar para brindarse durante la prestación del servicio y estas deben estar plasmadas en el plan de trabajo que se debe

presentar al inicio de la ejecución del contrato.

3. CARACTERÍSTICAS TÉCNICAS PARA LA IMPLEMENTACIÓN:

- Realizar un plan de trabajo y/o cronograma de actividades, concertado con el supervisor, en un término no mayor a cinco (5) días hábiles posteriores a la firma del acta de inicio.
- Configuración y alistamiento de la solución a la última versión estable aprobada por el fabricante.
- Implementación de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.
- Pruebas de funcionamiento del servicio.
- Puesta en Producción del servicio.
- Configuración y estabilización del servicio.
- Entrega de la solución a satisfacción de la entidad.
- Dentro de los servicios se debe tener en cuenta la instalación, configuración y puesta en producción de las soluciones ofertadas, así como la estrega a satisfacción de estos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que alguna de estas genere costos adicionales para la entidad.
- Las actividades de instalación, configuración y puesta en producción del servicio deberán serrealizadas por personal certificado por el fabricante.
- Se debe garantizar la usabilidad en diferentes entornos de nube.

BRUCE VARGAS VARGAS JEFE OFICINA TIC

Elaboró Asp Técnicos: David Quintero Rodríguez – Contratista OTIC V/B
Paula Andrea Moreno Ibarra – Contratista OTIC
Revisó: Juan José Olivella Crespo – Profesional Especializado