UNIVERSIDAD INDUSTRIAL DE SANTANDER
DTIC

TÉRMINOS DE REFERENCIA
PRELIMINAR

VOLUMEN II: ESPECIFICACIONES TÉCNICAS
CONVOCATORIA PÚBLICA ABREVIADA No. 14 de 2026

SUMINISTRO DE UNA SOLUCIÓN DE PROTECCIÓN DE APLICACIONES WEB (WAF) EN MODALIDAD HÍBRIDA (CLOUD Y COMPONENTE LOCAL DESPLEGADO EN LA INFRAESTRUCTURA INSTITUCIONAL) PARA PROTEGER LOS SERVICIOS WEB INSTITUCIONALES DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.

DIVISIÓN DE CONTRATACION
ABRIL DE 2026

Contenido

1. INTRODUCCION

La Universidad Industrial de Santander, en el marco de su estrategia de fortalecimiento de la seguridad de la información y la protección de sus servicios tecnológicos institucionales, requiere la implementación de una solución integral de protección de aplicaciones web (WAF), que permita mitigar los riesgos asociados a amenazas en capa de aplicación y garantizar la disponibilidad, integridad y confidencialidad de los servicios expuestos.

El crecimiento de los servicios digitales institucionales, así como el incremento de amenazas cibernéticas dirigidas a aplicaciones web, hace necesario contar con mecanismos avanzados de protección que permitan identificar, prevenir y responder de manera oportuna ante intentos de explotación de vulnerabilidades, ataques automatizados y otros eventos de seguridad.

En este contexto, se requiere la adquisición de una solución WAF en modalidad híbrida, que combine capacidades de protección en la nube y componentes locales, permitiendo una cobertura integral tanto para servicios expuestos a Internet como para aplicaciones internas. Esta solución deberá integrarse con la infraestructura tecnológica existente de la Universidad, optimizando el uso de recursos disponibles y facilitando su operación.

Así mismo, la solución deberá garantizar altos niveles de disponibilidad, visibilidad y control, incorporando funcionalidades que permitan la gestión centralizada, el monitoreo continuo y la generación de alertas y reportes, contribuyendo a la mejora continua de la postura de seguridad institucional.

La presente especificación técnica establece los requisitos mínimos que deberán cumplir los proponentes interesados en participar en el proceso de selección, con el fin de asegurar la adquisición de una solución robusta, escalable y alineada con las necesidades actuales y futuras de la Universidad.

2. OBJETO

Suministro de una solución de protección de aplicaciones web (WAF) en modalidad híbrida (cloud y componente local desplegado en la infraestructura institucional) para proteger los servicios web institucionales de la Universidad Industrial de Santander.

3. ALCANCE

La solución deberá:

- Proteger aplicaciones web institucionales expuestas a Internet y servicios internos.
- Implementarse bajo un esquema híbrido, que incluya:
    - Protección externa (cloud)
    - Protección interna (on-premise o equivalente)
- Permitir la protección de mínimo diez (10) subdominios institucionales, con capacidad de ampliación sin cambio de plataforma.

4. ARQUITECTURA DE LA SOLUCIÓN

La solución deberá:

- Operar bajo un esquema híbrido integrado, combinando componentes en la nube y componentes locales.

- Permitir la gestión centralizada de políticas, integración entre sus componentes y continuidad del servicio.
- Permitir la integración y gestión de configuraciones y eventos tanto en el componente cloud como en los componentes locales, mediante un plano de control único o mecanismos equivalentes definidos por el fabricante, de forma transparente.

El proponente podrá implementar la solución conforme al modelo arquitectónico propio del fabricante, siempre que cumpla con los requerimientos definidos.

5. REQUERIMIENTOS TÉCNICOS MÍNIMOS

5.1 Capacidades generales

- Protección contra vulnerabilidades tipo OWASP Top 10.
- Protección contra ataques DDoS a nivel de aplicación (capa 7).
- Protección de APIs.
- Detección de tráfico automatizado (bots).
- Capacidades de inteligencia de amenazas que permitan identificar y mitigar tráfico malicioso, mediante el uso de información de reputación, análisis de comportamiento u otras técnicas equivalentes.
- Inspección de tráfico HTTP y HTTPS.
- Capacidad de análisis de tráfico en tiempo real (runtime).

5.2 Protección externa (cloud)

- Capacidad de mitigación distribuida de ataques.
- Protección frente a tráfico malicioso proveniente de Internet.
- Capacidad de protección frente a variaciones en el volumen de tráfico, asegurando la continuidad del servicio sin degradación.

5.3 Protección interna (componente local)

La solución deberá incluir un componente local desplegado en la infraestructura institucional, en modalidad virtual o equivalente, que permita:

- Integración con la red institucional.
- Protección, gestión o procesamiento de tráfico interno, de acuerdo con la arquitectura del fabricante.
- Operación integrada con el componente cloud.

5.4 Descubrimiento y protección de APIs

- Protección de endpoints API.
- Capacidad de análisis y clasificación de tráfico asociado a APIs, que permita identificar comportamientos anómalos o riesgos asociados.
- Opcionalmente, la solución podrá incluir capacidades de identificación, inventario y perfilamiento de APIs, incluyendo APIs no documentadas o “Shadow APIs”.

5.5 Visibilidad y monitoreo
La solución deberá incluir:

- Consola centralizada de administración.
- Visualización unificada de eventos de seguridad asociados a tráfico web, APIs, bots y ataques de denegación de servicio (DDoS) en tiempo real.
- Generación de reportes.
- Configuración de alertas.

5.6 Logs y trazabilidad

- Registro de eventos de seguridad.
- Acceso a logs de tráfico y ataques.

La solución deberá incluir, dentro de la oferta presentada, todas las capacidades necesarias para el acceso, consulta y análisis de logs de tráfico y eventos de seguridad, sin restricciones que limiten la gestión operativa de la Universidad.

5.7 Alta disponibilidad
La solución deberá garantizar mecanismos de alta disponibilidad y continuidad del servicio, asegurando la operación de los servicios protegidos ante fallas o eventos adversos.

5.8 Capacidades avanzadas de protección

La solución deberá incluir capacidades avanzadas de protección que permitan la detección y mitigación de ataques conocidos y desconocidos, incluyendo aquellos de día cero, mediante mecanismos de análisis de comportamiento, correlación de eventos o tecnologías equivalentes.

La solución deberá permitir la identificación y gestión de falsos positivos mediante ajuste de políticas, creación de excepciones controladas y mecanismos de afinamiento.

La solución deberá soportar la integración y gestión de certificados digitales utilizados por las aplicaciones protegidas.
La solución deberá permitir la protección granular de aplicaciones web, incluyendo control y validación de accesos a nivel de rutas, URLs o endpoints.

La solución deberá incluir mecanismos de identificación y bloqueo de fuentes de tráfico malicioso, mediante el uso de inteligencia de amenazas, análisis automatizado o tecnologías equivalentes.

La solución deberá contar con capacidades de detección de amenazas en el lado del cliente (client-side), incluyendo monitoreo de scripts, identificación de comportamientos anómalos o riesgos asociados a la cadena de suministro de JavaScript.

La solución deberá incluir capacidades de mitigación de ataques de denegación de servicio (DDoS), con capacidad suficiente para soportar escenarios de tráfico malicioso sin degradación del servicio.

6. IMPLEMENTACIÓN

El proponente deberá incluir en su propuesta:

- Instalación de la solución.

- Configuración inicial.
- Integración con la infraestructura institucional.
- Puesta en producción.
- Acompañamiento en fase de estabilización.

El proponente deberá garantizar que la implementación de la solución se realice de manera compatible con la infraestructura tecnológica existente de la Universidad, optimizando el uso de recursos, minimizando impactos operativos y garantizando la continuidad del servicio durante la implementación.

7. SOPORTE TÉCNICO

La solución deberá incluir servicios de soporte técnico por un periodo de tres (3) años contados a partir de la entrega en operación de la solución, cumpliendo como mínimo con lo siguiente:

- Soporte técnico en modalidad 7x24.
- Atención de incidentes, requerimientos y solicitudes de servicio.
- Soporte local o remoto a través del proponente.
- El tiempo de respuesta máximo (telefónica o conexión remota) ante solicitudes de soporte por parte de la universidad no deberá exceder las dos (2) horas.
- Los tiempos de solución para las solicitudes de soporte de la Universidad relacionadas con la solución objeto del contrato, de máximo tres (3) horas para incidentes críticos y de máximo dos (2) días hábiles para las demás solicitudes, contados a partir de su registro o notificación.

El proponente será el responsable integral de la prestación del soporte, actuando como punto de contacto ante la Universidad, y deberá garantizar la gestión, seguimiento y resolución de los casos reportados.

El proponente deberá garantizar el respaldo y soporte del fabricante de la solución, incluyendo acceso a actualizaciones, firmas de seguridad y asistencia técnica especializada.

El esquema de soporte deberá contemplar servicio técnico especializado durante la vigencia del periodo de soporte solicitado, garantizando cobertura continua en la atención de incidentes.

En ningún caso el modelo de soporte ofrecido deberá generar restricciones que afecten la atención de incidentes críticos ni la continuidad operativa de la solución.

8. LICENCIAMIENTO

La solución deberá:

- Ser suministrada bajo modalidad de suscripción por tres (3) años.
- Incluir:
    - Todas las funcionalidades ofertadas.
    - Actualizaciones.
    - Soporte.

- Acceso a logs y monitoreo.

9. CONTINUIDAD DEL SERVICIO

Dado que la Universidad cuenta actualmente con una solución WAF en operación, el proponente deberá:

- Garantizar la continuidad del servicio.
- Evitar interrupciones durante la implementación o migración.
- Presentar plan de transición, si aplica.

10. ENTREGABLES

El proponente deberá entregar:

- Documentación de la solución implementada.
- Arquitectura desplegada.
- Manuales de operación.
- Configuración inicial aplicada.
- Transferencia de conocimiento