ANEXO TÉCNICO

ESPECIFICACIONES TÉCNICAS MÍNIMAS

Objeto:

PRESTAR EL SERVICIO DE WAF EN NUBE Y SOPORTE TÉCNICO PARA PROTECCIÓN DE LAS APLICACIONES WEB DE LA SECRETARÍA DISTRITAL DE MOVILIDAD.

ALCANCE

SERVICIO WAF	
Características	**Requerimiento Mínimo**
Servicio	Un servicio de Waf en Nube para la protección de las aplicaciones web definidas por la entidad, incluyendo la implementación, configuración, puesta en operación, soporte y acompañamiento técnico requerido durante la ejecución contractual.
Aplicaciones	El servicio se debe dimensionar para proteger un total de mínimo 20 aplicaciones.
Ancho de Banda	El servicio se debe dimensionar teniendo en cuenta que el tráfico legítimo hacia las aplicaciones será de máximo 350 Mbps.
SOPORTE TÉCNICO	
El servicio debe incluir soporte técnico 7*24*365, durante toda la vigencia contractual. El soporte deberá prestarse mediante los siguientes canales de atención: chat, portal web o mesa de servicio, correo electrónico y atención telefónica.	

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
GENERALIDADES	La solución deberá permitir la protección de las aplicaciones web de la entidad frente a amenazas externas, conforme al alcance contratado.
	La solución deberá permitir la administración e implementación de políticas de seguridad de manera centralizada y segura.
	La solución debe estar en capacidad de proteger aplicaciones web sin importar su ubicación (en premisas o en nubes públicas o en nubes privadas).
	El servicio deberá ser compatible con IPv6.

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
	La solución deberá contar con consola de administración web con acceso cifrado mediante HTTPS.
CARACTERÍSTICAS DE PROTECCIÓN DE APLICACIONES	La solución deberá contar con capacidades para detectar, prevenir, alertar, mitigar y/o bloquear amenazas dirigidas a aplicaciones web, mediante mecanismos nativos de la solución, tales como firmas, análisis de comportamiento, reputación, validación de protocolo, aprendizaje automático u otros mecanismos equivalentes.
	Como mínimo, la solución deberá brindar protección frente a amenazas asociadas a: Cross-Site Scripting (XSS) SQL Injection Cross Site Request Forgery (CSRF) Remote File Inclusion Local File Inclusion Inyección de Comandos Protección contra Exposición o fuga de información sensible. Manipulación maliciosa de cabeceras HTTP, HTTP header overflow,XML o JSON malformado Ataques automatizados sobre formularios o portales de autenticación. Bots maliciosos, crawlers no deseados y tráfico automatizado anómalo. Alteración o reutilización indebida de cookies o sesiones. Abuso, explotación o uso malicioso del protocolo HTTP/HTTPS
	La solución deberá permitir la habilitación y configuración de políticas basadas en los estándares HSTS, CSP, X-Frame-Options, X-XSS-Protection y Referrer-Policy para la protección de ataques: ● Ataques de degradación de HTTPS a HTTP ● Sniffing (escucha) de tráfico ● Inyección de código malicioso (JavaScript, CSS, iframe, etc.). ● Clickjacking (ocultar una página dentro de un iframe para engañar al usuario y hacer clic donde no quiere). ● Filtración de datos sensibles a través de la cabecera Entre otros.
	La solución deberá contar con mecanismos para detectar y mitigar ataques de fuerza bruta, relleno de credenciales, bots maliciosos, crawling abusivo y otros intentos repetitivos o automatizados de acceso no autorizado.

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
	La solución deberá permitir detectar, clasificar y mitigar tráfico automatizado malicioso, incluyendo bots no deseados, scraping abusivo, crawlers maliciosos o intentos automatizados de explotación.
	La solución deberá permitir el uso de listas blancas y listas negras basadas en dirección IP de origen, así como mecanismos de reputación de IP con actualización automática.
CARACTERÍSTICAS DE DETECCIÓN AVANZADA	La solución debe contar con métodos de detección de ataques que no estén basados únicamente en firmas, sino que incorpore mecanismos complementarios para identificar comportamientos anómalos o amenazas emergentes; tales como: Inteligencia Artificial (IA) y Machine Learning (ML) basados en modelos matemáticos y probabilísticos que permitan recolectar, aprender, probar y regenerar los datos que deben ser aceptados en los parámetros del sitio web protegido.
	La solución debe aprender de forma automática los métodos usados en los sitios web protegidos, con el fin de mejorar la detección de anomalías y reducir falsos positivos y falsos negativos.
	La solución debe contar con motores de Inteligencia Artificial (IA) y/o Machine Learning (ML), uno para la detección de anomalías en los parámetros protegidos y el otro que identifique ataques en los mismos.
	El servicio debe soportar utilizar servicios adicionales de inteligencia del fabricante para incrementar el nivel de protección ante amenazas avanzadas.
	La solución debe permitir detectar comportamientos automatizados o no humanos mediante señales del cliente, desafíos técnicos o mecanismos equivalentes.
	La solución debe proteger contra ataques de día cero basados en aprendizaje automático, análisis de comportamiento.
CARACTERÍSTICAS MÍNIMAS DE PROTECCIÓN DoS	La solución deberá contar con capacidades para prevenir, detectar y mitigar ataques de denegación de servicio a nivel de aplicación o sobre HTTP/HTTPS o a nivel de aplicación, mediante acciones como alertar, denegar y bloquear por un tiempo determinado.

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
CARACTERÍSTICAS DE GEOLOCALIZACIÓN	El servicio deberá contar con capacidades de protección, restricción o bloqueo basadas en la localización geográfica del origen del tráfico.
CARACTERÍSTICAS DE INTEGRACIÓN	La solución deberá poder integrarse con ambientes de nube pública (al menos AWS y Azure), así como con infraestructuras administradas por la entidad o por terceros autorizados, cuando ello resulte necesario para la continuidad del servicio.
	La solución deberá permitir, cuando aplique, la actualización de parámetros de direccionamiento hacia orígenes o servidores de aplicación cuyo direccionamiento cambie dinámicamente.
VALIDACIÓN DE PROTOCOLO Y CONTENIDO	La solución deberá validar el protocolo HTTP/HTTPS y,, permitir validación de estructuras o esquemas como OpenAPI, XML y JSON, así como definir acciones frente a anomalías o eventos sospechosos detectados.
PROTECCIÓN DE APLICACIONES WEB Y APIs	La solución deberá proteger aplicaciones web y APIs, así como permitir interoperabilidad con especificaciones OpenAPI 3.0 o equivalentes.
GESTIÓN DEL TRÁFICO WEB	La solución deberá permitir la administración de políticas de seguridad para tráfico HTTP/HTTPS.
	La solución deberá permitir bloquear métodos HTTP no autorizados o no requeridos.
	La solución deberá permitir definir límites o restricciones al tamaño de archivos cargados.
	La solución deberá permitir redirigir tráfico HTTP a HTTPS.
	La solución deberá permitir realizar reescritura o transformación controlada de solicitudes o respuestas HTTP, cuando la necesidad técnica lo justifique.
	La solución deberá permitir insertar encabezados requeridos por la arquitectura, incluyendo X-Forwarded-For o equivalentes, cuando aplique.
	La solución deberá permitir direccionar tráfico hacia orígenes, servicios o aplicaciones específicas con base en criterios configurables.
	La solución deberá permitir definir reglas para aceptar, restringir, bloquear o limitar solicitudes con base en URL, origen, comportamiento o tasa de consumo.

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
CARACTERISTICAS DE ADMINISTRACION Y MONITOREO	El servicio debe contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, amenazas, peticiones bloqueadas e información de licenciamiento.
	El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS.
	Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema.
	La configuración de administración de la solución debe permitir la utilización de perfiles, roles y privilegios diferenciados.
	Debe ser capaz de realizar notificaciones de eventos de seguridad a través de Syslog.
	La solución deberá permitir análisis en tiempo real e histórico del tráfico y de la actividad asociada a amenazas o bots.
SERVICIOS PROFESIONALES	El contratista deberá incluir, como parte integral del servicio, las actividades de: Implementación, configuración, pruebas y puesta en marcha del servicio ofertado.
	Las actividades de implementación deberán ser ejecutadas por personal con competencias y/o certificaciones vigentes relacionadas con la solución ofertada.
REQUERIMIENTOS DE IMPLEMENTACIÓN	La ejecución de las actividades de implementación iniciará una vez el supervisor del contrato apruebe el equipo de trabajo presentado por el contratista.
	Las actividades de implementación deberán planearse y validarse en conjunto con la entidad.
	Se debe realizar el levantamiento de requerimientos técnicos y configuración inicial del servicio.
	Se debe ejecutar pruebas funcionales de las aplicaciones que pasarán por el waf antes de su paso a producción.
	Configuración y estabilización del servicio ofertado.
	Se deberá presentar al supervisor del contrato, dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, el cronograma detallado de ejecución para la implementación del servicio.
	La implementación y entrega del servicio a satisfacción de la Entidad no podrá superar quince (15) días hábiles, contados a

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
	partir de la entrega del cronograma detallado de ejecución.
REQUERIMIENTOS DE SOPORTE	El contratista deberá garantizar soporte para el servicio ofertado en un esquema 7 x 24 x 365.
	El servicio de soporte debe incluir atención de requerimientos técnicos de operación, administración, configuración e incidentes asociados al servicio ofertado.
	Prestar soporte por vía telefónica, por e-mail, chat o mesa de servicio, portal web y realizar el escalamiento de casos con el fabricante, en caso de requerirse durante el tiempo del servicio WAF.
	Sesiones remotas de soporte, para atención de requerimientos realizados o por fallas y afectación del servicio WAF hacia las aplicaciones de la SDM.
AUTENTICACIÓN DEL PORTAL DE ADMINISTRACIÓN	La solución debe soportar mecanismos de autenticación robusta para el acceso al portal de administración, incluyendo como mínimo autenticación multifactor (FA).
EQUIPO DE TRABAJO	Para la ejecución del contrato se requieren los siguientes perfiles los cuales deben ser presentados por el contratista dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, para revisión y aprobación del supervisor de de conformidad con lo establecido a continuación: **Gerente de Proyecto** Un (1) profesional en Ingeniería de Sistemas o Electrónica o Eléctrica o de Redes o de Telecomunicaciones o áreas afines. Deberá contar como mínimo con una Especialización y/o Maestría en áreas relacionadas con TI y/o certificación PMP vigente. Deberá acreditar experiencia profesional general mínima de cinco (5) años y experiencia específica como Coordinador de Proyectos y/o Gerente de Proyectos y/o Líder de Proyectos y demostrar al menos dos (2) años en proyectos de implementación de servicios relacionados con el objeto contractual, contados a partir de la fecha de expedición de la tarjeta profesional. **Profesional en Ingeniería o Afines**

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195

ESPECIFICACIONES TÉCNICAS GENERALES	
Características	**Requerimiento Mínimo**
	Un (1) profesional en Ingeniería de Sistemas o Electrónica o Eléctrica o de Redes o de Telecomunicaciones o en áreas afines, quien desempeñará el rol de líder implementador. Deberá contar como mínimo con la certificación vigente del fabricante del servicio ofertado. Deberá acreditar experiencia profesional mínima de cinco (5) años en implementación y/o soporte y/o mantenimiento de soluciones waf contados a partir de la expedición de la tarjeta profesional.

Acuerdos de Niveles de Servicio SLA Servicio de Soporte Técnico 7*24*365			
Criticidad	**Descripción**	**Tiempo Respuesta Máx.**	**Tiempo Solución Máx.**
Crítica	Servicio WAF- Inoperativo	15 minutos	4 horas
Alta	Bloqueo tráfico legítimo masivo	30 minutos	8 horas
Media	Falsos positivos afectando usuarios	1 hora	24 horas
Baja	Consultas/Optimización reglas	4 horas	3 días hábiles

Elaboró:

Estructuradores Técnicos

Jasvleidy Fajardo Rozo--Profesional Especializado-Estructurador Técnico-OTIC

Elsa Marlen Baracaldo Huertas-Contratista-Estructurador Técnico-OTIC

Secretaría Distrital de Movilidad
Calle 13 # 37 - 35
Teléfono: (1) 364 9400
www.movilidadbogota.gov.co
Información: Línea 195