BILBAOTIK, S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL DESPLIEGUE DE UN WAF PARA EL CONTROL DE APLICACIONES WEB PERIMETRALES

Julio de 2025

1.- Objeto del contrato

BilbaoTIK gestiona la operativa de seguridad de la red municipal y para ello ha de dotarse de soluciones que permitan proteger las personas, infraestructuras y aplicaciones de forma adecuado. En este contexto, se plantea avanzar en la protección en capa 7 de las aplicaciones expuestas a redes públicas, llevando su primera barrera de seguridad a un formato cloud, tal y como ya se viene haciendo con otras muchas plataformas. Con ello, se trata de minorar la prevalencia de los ataques de tipo DDoS, muy complejos de defender con medidas basadas únicamente en on premise.

El objeto del presente contrato es la adquisición y puesta en marcha de nuevos mecanismos de protección en capa 7 para todas las aplicaciones y APIs municipales.

2.- Alcance y descripción del contrato

De forma más detallada, el objeto del contrato es la adquisición, despliegue, configuración y puesta en servicio de una solución de cortafuegos de aplicaciones web en modalidad de servicio en la nube (SaaS). El objetivo principal es permitir la simplificación de la publicación e implantación de controles de seguridad mínimos y comunes para todo el ecosistema de aplicaciones.

La plataforma seleccionada deberá integrarse de manera transparente con la infraestructura y soluciones de seguridad existentes (en lo que respecta a este punto, fundamentalmente firewalls Check Point y balanceadores F5), reforzando la postura de seguridad general.

Arquitectura

Servicio basado en SaaS, que contará con los siguientes componentes:

- Una red global de puntos de presencia del proveedor de servicio (nodos públicos) consumida como servicio para la publicación y protección de aplicaciones, con las siguientes características:
    - Punto de presencia en España.
    - Puntos de presencia instalados y operados por el proveedor SaaS con todos los PoPs publicándose mediante IPs ANYCAST para garantizar la disponibilidad global.
    - Los PoPs (nodos públicos) del proveedor no pueden ejecutarse en ninguna nube pública para evitar la dependencia del SLA de los proveedores de nube.
    - Capacidad de ofrecer los servicios a través de IPs propiedad de BilbaoTIK (Bring Your Own IP)
- Aunque no se requiere inicialmente, capacidad de extender todas las funcionalidades descritas mediante la instalación de nodos privados en las instalaciones de BilbaoTIK (o

cualquier tenant privado en nubes públicas o privadas) para la publicación y protección de las aplicaciones privadas, soportando al menos los siguientes modos de instalación:

- Implementación Baremetal en hardware propietario del proveedor (sujeto a validación de Hardware certificado)
- Implementación de VM en hipervisor (VMWare, KVM)
- Implementación de máquinas virtuales en la nube pública (AWS, GCP, Azure)
- Implementación de pods en cluster de Kubernetes

Cuando se despliegue en entornos de nube pública, la solución propuesta deberá tener una integración directa de API con AWS, GCP, AZURE, para adjuntar sus VPC/VNET con la red SAAS de forma privada.

- Ofrecerá un portal de administración único que permitirá la gestión, configuración, visibilidad, además del análisis de la publicación y protección de las aplicaciones, ya sea en nodos del proveedor o en nodos privados del cliente. Entre sus principales características se incluyen:
  - Abstracción total de los recursos y la infraestructura existente, permitiendo tener las cargas de la aplicación en un centro de datos privado, público o combinación de estos.
  - No será necesario instalar agentes o componentes software dentro de las propias aplicaciones.

Se requerirá de forma expresa el acceso a todos los paneles de configuración y administración de la plataforma con plena autonomía a todos los niveles, por lo que los servicios gestionados que no permitan el acceso a la consola no cumplirán los requerimientos.

Publicación de Aplicaciones

La plataforma SaaS tendrá la capacidad de publicación de aplicaciones de manera independiente a cómo se ejecuten, desde donde se ejecuten y desde dónde se acceda a estas.

La solución deberá soportar las siguientes funcionalidades:

- Publicación de servicios a través de la infraestructura del proveedor sin limitación en el ancho de banda. El servicio deberá tener la capacidad de integrarse de manera nativa con el equipamiento BIG-IP ya existente para el descubrimiento de servicios que se encuentren detrás de Virtual Servers para utilizarlos como destino final de los servicios publicados.
- Publicación de al menos 32 FQDNs

- Volumen de peticiones hasta al menos 30 millones de peticiones mensuales
- Balanceo de tráfico de nivel 4 y nivel 7
- Enrutado de contenido basado en características de nivel 4 y 7 de las peticiones.
    - Se podrán definir en base al método y la coincidencia de ruta pudiendo definir los patrones como prefijo, ruta exacta y expresión regular.
    - Se podrán realizar reescrituras de host, inserción de encabezado de solicitud y respuesta, redirigir a un origen diferente, adjuntar diferentes políticas de WAF por ruta y manipular los encabezados de solicitud y respuesta.
- Balanceo distribuido entre varias instancias de la misma aplicación pública existentes en diferentes localizaciones.
    - La decisión de balanceo se tomará en el nodo público más cercano al usuario.
- Especificación del servidor de origen de la aplicación basado en:
    - Nombre DNS público del servidor de origen
    - Dirección IP privada del servidor de origen (conectado a través un nodo privado)
    - IP pública del servidor de origen
    - Nombre privado DNS del servidor de origen en un sitio (conectado a través una instalación privada)
    - Nombre del servicio de Kubernetes del servidor de origen en un sitio (conectado a través una instalación privada sobre Kubernetes)
    - Nombre de servicio descubierto a través de la integración nativa con BIG-IP (conectado a través una instalación privada)
- Soporte de redirección del tráfico de aplicaciones públicas mediante CNAME, y mediante delegación de dominios en el propio servicio.
- Personalización de la conexión TLS tanto en el tramo cliente - PoP como en el tramo POP-Servidor de origen. Esta personalización debe incluir al menos la selección de SNI, el nivel de seguridad, la verificación del servidor de origen y MTLS
- Publicación de las aplicaciones web y APIs públicas mediante IP anycast a nivel global.
- Configuración del tiempo de espera de conexión para las conexiones TCP
- Configuración del tiempo de espera de inactividad HTTP

- Activación o desactivación del protocolo HTTP2 en la comunicación con el servidor de origen.
- Capacidad de configurar más de un nombre de dominio para una aplicación publicada HTTP/HTTPS
- Publicación de servicios HTTP y HTTPS en puertos de destino no estándar (distintos de los puertos 80 y 443)
- Disyuntor (Circuit Breaker): esta funcionalidad deberá proporcionar mecanismos para observar fallos en las conexiones o solicitudes enviadas a los servidores de origen y, si los fallos alcanzan un cierto umbral, hacer fallar automáticamente las solicitudes posteriores, lo que ayudará a determinar si algunos hosts en un clúster tienen un rendimiento diferente a otros (como dar más respuestas 5xx a solicitudes genuinas, etc.) y eliminarlos de los conjuntos de servidores de origen utilizados para el equilibrio de carga.
- Generación automática de certificados para servicios publicados.
- Compatible con certificados generados mediante entidades de certificación de terceros o locales. Capacidad de almacenar las claves privadas de los certificados en un servicio de gestión de secretos propietario e incluido en el servicio.
- Definición de perfiles TLS personalizados con versiones de TLS específicas y conjuntos de cifrado específicos según necesidades.
- Definición de una página de respuesta específica a los clientes que acceden a la aplicación web en caso de códigos de respuesta 4xx, 5xx del servidor de origen.
- Capacidad futura de extender la solución para soportar la carga y ejecución de aplicaciones basadas en microservicios en los nodos privados y gestionarlo desde la misma consola.

Seguridad Web y APIs

El servicio deberá proporcionar una plataforma única con capacidad de controlar el nivel de seguridad de todas las aplicaciones, independientemente de:

- Cómo hayan sido desarrolladas (servidor de aplicaciones, contenedores, etc.)
- Desde dónde se estén ejecutando
- Si están siendo entregadas de manera pública en Internet o de manera privada

El servicio de seguridad de aplicaciones tendrá las siguientes características:

- Los controles de seguridad se podrán definir de manera centralizada en una consola única de servicio que permitirá el despliegue de políticas comunes de seguridad para las aplicaciones públicas y privadas.
- Análisis en línea, donde todo el tráfico hacia las aplicaciones públicas entre a través de los nodos públicos del proveedor, deteniendo los ataques antes de llegar a la aplicación web o API protegida.
- Capa de protección básica de aplicaciones que incluya al menos:
    - Protección DDoS a nivel de red y de capa de aplicación
    - WAF (Web Application Firewall): violaciones de protocolo, vulnerabilidades, reputación de IPs para un volumen mínimo de 30 millones de peticiones mensuales.
    - Deberá estar alimentado con servicios de inteligencia del proveedor para la detección y mitigación de campañas de ataques activas.
    - Políticas de servicio (ACLs avanzadas de nivel 7).
    - Protección de APIs (para al menos 1 API y 500k peticiones al mes)
        - Descubrimiento dinámico de API Endpoint basado en tráfico (sin necesidad de elementos externos fuera de banda). Descarga de los esquemas descubiertos dinámicamente.
        - Descubrimiento estático de API Endpoint basado en la importación de fichero Swagger
        - Descubrimiento estático de API Endpoint basado en el escaneo de repositorios de código
        - Detección de tipo de autenticación en los API Endpoints
        - Detección de información sensible intercambiada por los API Endpoints
        - Detección de configuraciones de seguridad incorrectas en los API Endpoints y validación de los esquemas de las APIs
        - Limitación del número de peticiones a las APIs por origen, unidad de tiempo, etc.
        - Validación JWT
        - Establecimiento de políticas de rate limiting en función de parámetros de autenticación JWT
        - Detección de usuarios maliciosos: User Behavioural Analysis (UBA)

- Detección de bots basada en firmas

- Aunque no es requerido en este pliego técnico, deberá disponer de la capacidad de activar la protección antibot basado en IA (Opcional):
  - Funcionalidades antibot avanzadas basadas en AI/ML para detección de automatismos sofisticados con el objetivo de evitar situaciones de uso indebido da las aplicaciones que comprometen su seguridad

- Capacidad de enmascaramiento en vuelo de datos sensibles entre la plataforma y el usuario (por ejemplo, DNI o número de la Seguridad Social).

- El sistema SaaS deberá incluir conjuntos de firmas implementados out of the box (al menos 5.000), adicionales a los basados en implementaciones de firmas de código abierto como Modsec.
  - La plataforma SaaS debe tener flexibilidad para aplicar las firmas en función de la precisión en base a perfiles de cumplimiento: alta, media y baja.

- Permitirá la capacidad de definir la página de respuesta de bloqueo personalizada.

- Implementará el bloqueo de IPs según su reputación mediante una base de datos de reputación ofrecida por el proveedor.

- La plataforma SaaS deberá admitir el bloqueo de conexiones basadas en la IP de origen, el país, el número de asn, o el TLS fingerprint.

- La plataforma SaaS deberá admitir la capacidad de asociar varias políticas de WAF a la misma aplicación y aplicarlas en función del path/query string/cabecera.

- La plataforma SaaS admitirá un mecanismo de creación de reglas de exclusión de firmas fácilmente aplicable desde el registro de peticiones, que permita aplicar estas reglas sólo durante un tiempo determinado (para facilitar la remediación de este tipo de exclusiones de manera temporal para su solución definitiva mediante código de la aplicación).

- La plataforma SaaS deberá admitir la limitación de velocidad de peticiones (rate limiting) para al menos 10M de peticiones al mes

- La plataforma SaaS deberá permitir lanzar desafíos basados en JS y/o Captcha para hacer frente a los ataques DoS de capa 7

- La plataforma SaaS deberá admitir reglas para definir peticiones confiables para las que se omiten las comprobaciones de BOT y WAF

- La plataforma SaaS deberá ofrecer un servicio de escaneo de vulnerabilidades que permita evaluar la eficacia de las políticas de seguridad aplicadas, pero que permita

también evaluar otras aplicaciones que aún no estén siendo publicadas por la plataforma SaaS.

- Esta funcionalidad deberá ofrecerse integrada con la consola de administración única de la plataforma SaaS.
- La solución deberá realizar escaneos automatizados y periódicos, generando reportes detallados clasificados por nivel de criticidad para facilitar la remediación, permitiendo al menos 3 escaneos al mes.

Administración

La plataforma contará con una única consola de administración para la gestión de los nodos públicos y privados y todas las características, tanto las incluidas en la oferta del proveedor como las que se puedan incorporar posteriormente mediante ampliaciones. Sus funcionalidades mínimas serán las siguientes:

- Acceso a la consola mediante navegador
- Publicación de servicios a través de FQDNs
- Sistema de gestión de secretos (KMS)
- Definición de servidores origen basado en IP o en nombre DNS
- Comprobación de la disponibilidad de la aplicación
- Configuración de seguridad
- Visualización de analíticas por aplicación, al menos: métricas de tráfico por sitio web protegido con información acerca de latencias, eventos de seguridad, firmas encontradas, tipos de ataques automatizados, latencias entre usuario y aplicación, peticiones por segundo, ancho de banda, tasas de errores, tipos de navegadores, sistemas autónomos desde donde se accede y zonas geográficas. Descripción detallada de cada una de las peticiones HTTP recibidas, accesibles vía consola web o API.
- Cuadro de mandos unificado para aplicaciones privadas y públicas que mostrará, al menos: eventos de seguridad por tipo (WAF, bots, APIs o políticas de servicio), países de origen, eventos por países y paths más atacados.
- Gestión de logs, eventos de seguridad y granularidad para gestionar las políticas de seguridad de forma global o por aplicación.
- Soporte multi-usuario, con control de acceso basado en roles y espacios de trabajo independientes.
- Soporte de configuración programática basada en JSON y YAML a través de la interfaz gráfica

- Todas las opciones de administración serán accesibles también a través de APIs

DNS en la nube

La plataforma ofrecida deberá complementar sus servicios de publicación de aplicaciones con un servicio de DNS en la nube con las siguientes características:

- Incluirá la capacidad de configurar al menos 200 zonas DNS que se alojarán como DNS primario o DNS secundario.
- Implementará la firma de registros estáticos mediante DNSSEC
- Utilizará tecnología ANYCAST para ofrecer los servicios DNS
- Protegerá los servicios de DNS ante ataques DDoS
- Implementará la opción de autenticación TSIG
- Será compatible con IPV4/IPV6 Dual Stack
- Tendrá capacidad de configurar las siguientes características de los registros SoA:
    - Intervalo de actualización
    - Intervalo de reintento
    - Expiración
    - TTL negativo
    - TTL
- Tendrá capacidad de configurar registros DNS como:
    - A
    - AAAA
    - ALIAS
    - CAA
    - CNAME
    - MX
    - NS
    - RPP

- SRV
- TXT
- Contenido dinámico para balanceo GSLB
- APTR
- DS
- CDS
- EUI48
- EUI64
- AFS

- La plataforma SaaS deberá ser capaz de configurar el equilibrio de carga de DNS (GSLB)
- Deberá ser capaz de admitir la geolocalización
- Deberá ser capaz de realizar una inspección periódica de la salud de los miembros del pool
- Deberá ser capaz de especificar el TTL para los registros del equilibrador de carga
- Deberá ser capaz de admitir el almacenamiento en caché de respuestas

Servicios profesionales

El adjudicatario deberá proveer los siguientes servicios profesionales, considerados parte integral e indispensable de la solución durante todo el periodo del contrato. Cada uno de los servicios conllevará un informe de seguimiento mensual.

	Objetivo Principal	Entregables
Evaluación Inicial y supervisión continua	Optimización continua del WAF mediante un análisis del entorno. Revisión continua de la exposición a Internet para identificar posibles sitios web públicos no cubiertos	Informe de assessment, matriz de riesgos e informes de efectividad y rendimiento de las medidas.
Respuesta a Incidentes	Proporcionar capacidad de respuesta inmediata 24x7 ante amenazas detectadas en el WAF	Plan de Respuesta a Incidentes e informes post-incidente.
Inteligencia de Amenazas	Contextualizar la inteligencia para mejorar la efectividad de las políticas.	Reportes ejecutivos y alertas técnicas en tiempo real.
Auditorías y Pentesting	Validar continuamente la efectividad de las configuraciones de seguridad.	Informes técnicos de pentesting y plan de remediación.

Todos los trabajos se realizarán presencialmente en las oficinas de BilbaoTIK.

A modo de resumen, se incluyen los elementos objeto del contrato:

Elemento	Inicio
Licencias o suscripciones tecnológicas (3Y)	1 de noviembre de 2025
Servicios profesionales (3Y)	1 de noviembre de 2025

3.- Equipo de trabajo

El equipo de trabajo para la implantación y puesta en marcha constará, al menos, de 3 personas con un mínimo de 3 años de experiencia en el ámbito de la ciberseguridad, que se distribuirán de la siguiente manera:

- Una persona para la jefatura del proyecto. Deberá disponer de titulación universitaria superior en Ingeniería en Informática o Telecomunicaciones, valorándose estudios oficiales de especialización en ciberseguridad.
- Dos personas en el ámbito de la ciberseguridad. Al menos una de ellas deberá disponer de titulación universitaria superior.

La persona que actúe como jefe/a de proyecto tendrá entre sus funciones la interlocución operativa con BilbaoTIK.

Esta jefatura de proyecto se encargará de:

- Seguimiento de los niveles de servicio, índices de calidad y evaluación de los objetivos, de acuerdo con lo definido.
- Convocar las reuniones de seguimiento y cuantas reuniones estime oportuno para el correcto desarrollo de los trabajos.
- Coordinar los recursos humanos de la adjudicataria según los requerimientos del servicio.
- Elaborar el acta de las reuniones de seguimiento que se realizarán, como mínimo, mensualmente.
- Elaborar los informes técnicos y de servicio que se consideren oportunos.
- Emprender las acciones correctivas apropiadas, tras ser consensuadas con BilbaoTIK, en caso de detectarse desviaciones de calidad en el servicio.

Respecto al equipo de trabajo directamente asignado al proyecto también se tendrá en consideración lo siguiente:

- El equipo asignado deberá mantenerse durante todo el periodo de ejecución del contrato:
- La discrepancia entre el nivel de conocimientos técnicos del personal ofertado según valores especificados en la oferta, y los conocimientos reales demostrados en la ejecución de los trabajos, dará lugar el requerimiento a la adjudicataria de adopción de medidas para su corrección.
- Si la valoración de productividad y calidad de los trabajos de una persona del equipo se considera inadecuada, o resulten incidencias respecto a la correcta ejecución del servicio, se pondrá en conocimiento de la adjudicataria para adopción de medidas para su corrección.
- Si la empresa adjudicataria propusiera el cambio de una persona del equipo designada en la oferta lo comunicará por escrito con 15 días de antelación exponiendo los cambios realizados y adjuntará datos de perfil equivalente que adscribirá para sustitución.

Los medios humanos aportados por la contratista para la ejecución del contrato estarán sometidos al poder de dirección y organización de la adjudicataria en todo ámbito y orden legalmente establecido; será por tanto la adjudicataria la única responsable de dicho personal, no teniendo, por tanto, vinculación jurídico-laboral alguna con BilbaoTIK. Todo ello con independencia del control de la ejecución del contrato que corresponda.

El cumplimiento de lo previsto en esta cláusula, así como de los compromisos contenidos en su oferta respecto al equipo humano se considera obligación contractual esencial de forma que su incumplimiento por parte del contratista podrá ser causa de resolución del contrato.

Bilbao, a 15 de julio de 2025

BilbaoTIK Firmado digitalmente por MANUEL ROIBAL PRIETO - 22738555L Fecha: 2025.07.15 13:54:30 +02'00'

Manu Roibal Prieto
Director de Infraestructuras y Ciberseguridad
Responsable del contrato