



BILBAOTIK, S.A.

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA
CONTRATACIÓN DEL SERVICIO DE SOC (Centro de
operaciones de seguridad)**

febrero de 2025

1. OBJETO Y ALCANCE

BilbaoTIK puso en marcha un servicio de SOC durante el año 2023, como pieza vital en el mantenimiento de la seguridad corporativa municipal, consolidando todas las prácticas de análisis, detección y respuesta que se habían venido trabajando durante los últimos años. La renovación de este servicio es crítica para garantizar los niveles alcanzados en la seguridad IT.

El objeto de este expediente es la contratación del servicio de SOC durante un año, con una posible prórroga de otro año adicional.

2. DESCRIPCIÓN TÉCNICA DE LOS SERVICIOS

El Ayuntamiento de Bilbao debe hacer frente al creciente volumen y sofisticación de las amenazas. La falta de visibilidad de la red, el volumen de datos a analizar de los servicios ya implantados y la necesidad de filtrado y rápida respuesta en forma de alertas lleva consigo que ya no es posible hacer este análisis en forma manual. Por ello, se requiere automatizar los procesos y centralizar la gestión de seguridad de una forma que ayude a simplificar la difícil tarea de proteger la información que se maneja y el servicio que se presta.

Con la implantación de un sistema de gestión de eventos e información de seguridad se obtiene la recopilación de la información en tiempo real sobre los eventos de seguridad generados por la red para procesarla posteriormente con el fin de generar informes y/o alertas que puedan ayudar en la toma de decisiones en materia de seguridad. Este sistema se concibe como una plataforma de gestión de seguridad lógica de la red y se enfoca principalmente en los siguientes aspectos:

- Inventario y catalogación de activos.
- Gestión centralizada de los registros y eventos de seguridad generados por los sistemas.
- Análisis o monitorización en tiempo real de los eventos de seguridad de múltiples fuentes.
- Revisión manual (humana) de los positivos detectados para una mayor criba y eliminación de falsos positivos y notificación de la alerta, cuando proceda.
- Colaboración y asesoramiento técnico en la resolución de la incidencia derivada de la alerta

Además, se desea detectar los patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos. Para ello se implantarán sondas en la red de la entidad para recolectar la información de seguridad relevante y, después de un primer filtrado, enviar los eventos de seguridad hacia el sistema central que realiza una correlación entre los distintos elementos.

Los principales objetivos son los siguientes:

- Disponer de un método efectivo para automatizar los procesos y centralizar la gestión de seguridad de una forma que ayude a simplificar la protección de la información que se maneja y el servicio que se presta.
- Identificar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos, generando alertas según corresponda.

El SOC debe cumplir con las siguientes características básicas:

- Análisis de Big Data basado en la nube que permita el procesamiento y análisis de datos de registros de dispositivos de seguridad, infraestructura de red, y servidores y puestos de trabajo, para identificar eventos de interés.
- Monitorización de alertas 24x7x365, análisis, identificación y escalado de incidentes a través de fuentes de inteligencia de amenazas específicas de la industria.
- Equipos de analistas altamente cualificados que incluyen especialistas alineados con la organización de BilbaoTIK, analistas de seguridad certificados por GIAC, responsables de servicio e ingenieros de incorporación de activos y fuentes.
- Conjunto personalizable de procesos, incluida la escalada de incidentes de seguridad específica de BilbaoTIK y el ajuste individualizado de la gravedad del incidente.
- Detección anómala de tráfico, minería de datos y análisis estadístico para identificar actividades maliciosas previamente conocidas y desconocidas.
- Portal de cliente de panel unificado que proporcione una vista completa y orquestada de todos los incidentes de seguridad, dispositivos, activos e informes a través de un portal de autoservicio.
- Inteligencia de amenazas integrada que proporcione visibilidad de las amenazas que afectan a industrias, sectores y geografías específicas del cliente, incluidas herramientas, tácticas y procedimientos específicos de los atacantes, haciendo hincapié en aquellas que afecten específicamente al Ayuntamiento de Bilbao y sus entidades.
- Recopilación de todos los registros para su correspondiente análisis, sin eliminar registros considerados poco interesantes con el fin de reducir el coste de almacenamiento.
- Almacenamiento de registros extendido sin coste adicional, totalmente accesible, durante un período continuo de 12 meses.
- Eficacia contrastada con estadísticas que reflejen que la eficiencia y eficacia en la detección de casos reales y la no presencia de falsos positivos.

- Caza de amenazas retroactivas. A medida que se descubran nuevas amenazas e IOC significativos se volverán a procesar los últimos 30 días de los registros para garantizar que el entorno no se estaba comprometido antes de que la comunidad de seguridad identificara la amenaza.
- Casos de uso donde se mantengan y remedien los IOC publicados.
- Inteligencia procedente de múltiples fuentes, seleccionadas por un equipo global de inteligencia dedicado, para ayudar a aumentar las detecciones de auténticos positivos, incluyendo fuentes abiertas, paste bins, repositorios de código, fuentes cerradas y foros underground.
- Exploración, visualización y análisis de datos (DEVA) que proporcione visibilidad de los datos de registro para que los analistas puedan crear puntos donde pivotar, consultas de búsqueda anidadas, filtrado y paneles para proporcionar transparencia total de la postura de seguridad en todo momento.
- Conjunto de detección de análisis de comportamiento de personas y entidades (UEBA) construido mediante la base del comportamiento esperado, que permita a los equipos marcar actividades sospechosas y anómalas de personas y dispositivos.
- Interacción ilimitada con el equipo de servicio de SOC asignado, permitiendo entre otros mejorar la respuesta, la capacitación y el desempeño del equipo de BilbaoTIK.
- Análisis de la superficie de ataque y detección de vulnerabilidades en un conjunto de servidores considerados especialmente expuestos.
- Así mismo, análisis de la superficie de ataque y detección de vulnerabilidades en un conjunto de aplicaciones consideradas especialmente sensibles.

El proyecto se estructura en las siguientes fases:

- Fase de adquisición y puesta en marcha
- Fase de acompañamiento y soporte

2.1. Contenido del proyecto y especificaciones técnicas requeridas

2.1.1. Fase de adquisición y puesta en marcha

El proceso de Implantación propuesto estará orientado a reducir al máximo el tiempo de implantación del servicio estipulado, poniendo en marcha los servicios a medida que van estando disponibles.

No obstante, la adjudicataria propondrá la lista de servidores o sistemas a incluir, siempre tomando como base la lista anterior. Se priorizarán los eventos de los sistemas expuestos a redes públicas. Dentro de la plataforma existirá un mecanismo de inventario de activos y catalogación de estos.

Los logs no se enviarán directamente desde los sistemas, sino que se utilizarán elementos intermedios (colectores) proporcionados por la adjudicataria e instalados en la infraestructura del Ayuntamiento, bien como servidores físicos o virtuales sobre plataforma VMWare. Estos colectores se instalarán con mecanismos que preserven la disponibilidad ante caídas de equipamiento. En el SIEM se realizará el adecuado tratamiento de los datos mediante correlaciones y/o cualquier otra técnica estadística o basada en IA que permita la identificación de patrones de ataque.

El SIEM recogerá igualmente en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques sino, en la medida de lo posible, adelantarse a ellos para remediarlos antes de que sucedan.

La plataforma se alimentará igualmente de fuentes externas de vigilancia y alerta temprana, de forma que esta información se cruce con el inventario y eventos de la instalación de forma continua, con el objetivo de encontrar vulnerabilidades o ataques desde el primer momento en que se produzcan. Por tanto, la plataforma debe incluir un servicio de identificación de vulnerabilidades, tanto a nivel de infraestructura como de aplicaciones, que permita mantener un inventario de vulnerabilidades con actualización, como mínimo, diaria que permita contrastar la evolución de dichas brechas de seguridad. Igualmente, se alimentará el sistema con listas de IOCs con el mayor nivel de actualización posible.

Se estima un volumen de eventos inicial (mínimo a soportar) de 5.000 eventos por segundo con un posible crecimiento de un 20% anual. Se estima un volumen en torno a los 20 mil millones de entradas de log/eventos mensuales a enviar al SOC. Todos los logs del SIEM serán retenidos en los sistemas de la adjudicataria durante un mínimo de 12 meses en caliente (en los sistemas online), al tiempo que deberá existir un mecanismo simple y totalmente automatizado para que todos los eventos sean igualmente guardados en infraestructura municipal durante el tiempo que BilbaoTIK estime oportuno.

La adjudicataria propondrá los diferentes escenarios o caso de uso de los eventos recolectados en el SIEM, así como su posterior tratamiento.

Todas las alertas generadas por el motor SIEM deberán ser revisadas por un/a técnico/a de seguridad de la adjudicataria, como paso previo a su envío a BilbaoTIK. Esto deberá permitir con un importante nivel de acierto la eliminación de falsos positivos en la identificación de incidentes.

Toda la información recolectada junto a las posibles alertas generadas y el estado de salud global del sistema, así como el de cada uno de los elementos, deberá ser accesible mediante una consola centralizada que permita una gestión ágil.

Deberá incluirse un servicio de cibervigilancia que recopile contenido de fuentes amplias de información en línea, tales como fuentes abiertas de sitios web convencionales, paste bins,

repositorios de código, fuentes cerradas como sitios TOR o foros que requieren verificación antes de que se otorgue acceso: mercados dark web o foros underground y fuentes técnicas como sitios de análisis de malware o amenazas.

Todos los servicios descritos anteriores serán prestados desde la infraestructura de la adjudicataria, existiendo un túnel seguro entre ambas redes de forma que toda la información viaje en condiciones de máxima seguridad. Para ello se requerirá que el túnel sea establecido con los máximos niveles de seguridad en cuanto a protocolos y normativa.

Este proceso de adquisición y puesta en marcha no tendrá una duración superior a 1 mes, si bien, como se indicaba al inicio del apartado, se incentivará el despliegue progresivo a medida que cada pieza tecnológica va estando disponible. En definitiva, el objetivo no es esperar a la fecha final para desplegar todas las soluciones sino ir haciéndolo a medida que la planificación lo permite, extendiendo esta misma idea a cada una de las fases dentro de cada módulo.

A efectos de facturación, esta será mensual a medida que avance el proyecto de forma satisfactoria.

2.1.2. Fase de acompañamiento y soporte

Esta fase dará comienzo tras la finalización de la anterior y tendrá una duración de 11 meses.

El objetivo de esta fase es afinar el mecanismo de prestación de los nuevos servicios y de colaboración entre las partes. Para ello, se realizarán las mediciones de los indicadores, se emitirán los informes correspondientes con la periodicidad acordada (mínima de un mes) y se aplicarán las metodologías, procedimientos y actividades previstas en el modelo del servicio. Igualmente, durante este periodo se reportarán con la debida celeridad todas las alertas derivadas de incidentes de seguridad identificados por el sistema.

2.2 Otros requisitos

No se plantea la utilización de ningún servidor o recurso adicional a los indicados en este punto. Cualquier necesidad adicional deberá ser indicada de forma expresa e incluido dentro del alcance del proyecto.

A excepción de la infraestructura propia que por cuestiones técnicas o de negocio lo imposibiliten (donde la decisión última será de BilbaoTIK), y la que BilbaoTIK tenga que proveer para facilitar el acceso a la red de la adjudicataria, la provisión, instalación y todos los costes asociados de instalación y mantenimiento de las infraestructuras requeridas para la prestación del servicio, estarán a cargo de la adjudicataria, quien será la única responsable de su conservación y mantenimiento.

A modo de referencia, se facilitan algunos datos sobre volumetría de la red municipal:

Servidores (físicos y virtuales)	750
Puestos de trabajo	3.500
Retención mínima de los datos	12 meses en caliente
Eventos en pico	5.000 por segundo
Eventos/mensajes mensuales	20 mil millones

Todo el software y hardware objeto de esta licitación estará en mantenimiento y garantía hasta el final del proyecto. Todo el licenciamiento será con licencias que permitan una funcionalidad completa de los productos de acuerdo con la función para la que fueron desplegados, siempre durante el periodo de vigencia del proyecto.

La adjudicataria deberá formar parte de la Red de SOC Nacionales, además de formar parte de la red csirt.es y First. El equipo de trabajo propuesto deberá haber formado parte del equipo de la adjudicataria que haya desembocado en el cumplimiento de esos requisitos.

Asimismo, dada la especial sensibilidad de este proyecto respecto a la seguridad, la adjudicataria deberá acreditar la certificación ENS a nivel alto además de la ISO 27000.

2.3. Trabajos y cobertura horaria

Los servicios a realizar incluyen la recogida de datos, su análisis, catalogación y generación de alertas según corresponda. Este trabajo tiene su fundamento como servicio continuo en régimen de 24x7x365. Adicionalmente, la adjudicataria tendrá un equipo de trabajo que pueda apoyar al equipo de TI de BilbaoTIK en caso de requerir ayuda para la resolución de un problema técnico como consecuencia de una vulnerabilidad descubierta en la infraestructura. Este equipo estará en régimen de 24x7x365 para consultas con un tiempo máximo de atención de 2 horas.

Asimismo, se llevarán a cabo reuniones periódicas semanales de análisis de los resultados de los análisis anteriores, así como informe de recomendaciones de evolución de la seguridad municipal.

2.4 Requisitos de infraestructura tecnológica

Todo el servicio será realizado en formato cloud, salvo los conectores de información de cada servicio que estarán en los servidores origen, por lo que no hay una infraestructura requerida por parte de BilbaoTIK.

Los conectores deberán funcionar en sistemas Windows y Linux (RHEL, CentOS y Ubuntu), soportando middlewares y plataformas como, al menos, Active Directory, EDR de la

plataforma Falcon Crowdstrike, Jboss EAP, Tomcat, Websphere, IIS, Apache, Exchange on prem, SQL Server, MySQL, Oracle, Cisco Ironport, Big-IP, IPS module de Aruba, ProofPoint MTA, ForcePoint proxy, Checkpoint Firewall, Balanceadores F5, Controladoras WiFi de Aruba y electrónica de red de Aruba y Cisco.

2.5 Monitorización

En los servidores más expuestos en redes públicas o DMZ (hasta un máximo de 50 servidores) se instalará una herramienta de identificación de vulnerabilidades (qualsys o similar) que permita tener una foto en tiempo real de las vulnerabilidades existentes en cada máquina.

Asimismo, se hará un escaneo constante de hasta 50 sitios webs municipales (Bilbao.eus, webmail.bilbo.eus, urruti.bilbao.eus, bilbaokirolak.eus, ...) públicos o internos, haciendo un levantamiento general de todas las vulnerabilidades a nivel de aplicación, tanto en formato de caja negra como mediante la existencia de credenciales de acceso que permitan acceder a zonas internas de las aplicaciones.

3. METODOLOGÍA Y GESTIÓN DEL PROYECTO / SERVICIO

3.1. Dirección y equipo técnico del trabajo

Se formará un Comité para la dirección del proyecto, que estará compuesto al menos por la persona Responsable del Contrato designada por BilbaoTIK, una representante de la adjudicataria y cuantas otras personas designen las partes.

La misión de la persona responsable del contrato será la siguiente:

- a) Supervisar la ejecución del contrato.
- b) Asegurar la correcta realización de la prestación pactada, dictando las instrucciones y adoptando las decisiones necesarias para ello dentro de las facultades otorgadas por el órgano de contratación.
- c) En su caso, informar de los retrasos en la ejecución del contrato y realizar la propuesta para la aplicación de penalidades por incumplimiento parcial, cumplimiento defectuoso y demora en la ejecución.

Asimismo, BilbaoTIK designará una Dirección / Jefatura de Proyecto que tendrá entre sus funciones la planificación, seguimiento y control de los trabajos a realizar, así como la interlocución para la coordinación de los recursos humanos y disponibilidad de recursos materiales del mismo que sean necesarios en cada momento. BilbaoTIK controlará, mediante la figura mencionada, el cumplimiento de los términos acordados, así como la calidad y adecuación del servicio objeto de este expediente, en cuanto hace referencia a completar los términos y la calidad de los productos desarrollados. Sus funciones serán las siguientes:

- Autorizar los contactos directos de las personas del equipo de trabajo de la adjudicataria con personas de BilbaoTIK.
- Autorizar la entrega de documentación al Equipo de Trabajo de la adjudicataria.
- Autorizar el cambio de personas en el Equipo de Trabajo de la adjudicataria.
- Solicitar el cambio de personas del Equipo de Trabajo de la adjudicataria.

La Jefatura de proyecto o la persona en la que delegue, mantendrá reuniones de seguimiento con periodicidad como mínimo mensual.

El equipo de trabajo contará con el personal técnico adecuado y suficiente, que permita abordar con garantías el desarrollo del proyecto. Como mínimo, se deberán adscribir al contrato los siguientes perfiles:

Jefe/a de Proyecto

Máximo responsable de la correcta ejecución del proyecto y de la gestión y supervisión del mismo en base a las condiciones descritas en este pliego. Deberá contar con una experiencia probada mínima de 3 años en la implantación de SOC's en el ámbito de la Administración Pública. Las funciones que deberá desempeñar serán las siguientes:

- Controlar y gestionar los recursos del proyecto.
- Realizar y actualizar en cada fase el Plan de Proyecto (calendario, riesgos, tareas, recursos e involucración de los participantes).
- Monitorización del proyecto.
- Responsable de la organización interna del equipo de asistencia cuya responsabilidad prioritaria será la puesta a disposición del personal y medios auxiliares ofertados en la medida que sean demandados, así como la responsabilidad sobre los plazos de respuesta acordados.

Analistas de ciberseguridad

Experiencia probada mínima de 2 años en cada uno de los ámbitos de SOC (recolección, análisis, Ciberinteligencia, ticketing, ...) en implantaciones en el ámbito de la Administración Pública. Se deberá aportar información sobre el equipo de trabajo con soporte global 24x7, no siendo requerida la información particular de cada miembro del equipo de trabajo.

La empresa adjudicataria deberá garantizar y asegurar la capacitación técnica de las personas asignadas a la prestación de los servicios.

Todo el personal que preste los servicios objeto del presente contrato pertenecerá exclusivamente a la empresa adjudicataria del contrato, sin que exista ninguna relación jurídica

de tipo administrativo o laboral entre dichos/as trabajadores/as y BilbaoTIK, ni durante la vigencia del contrato ni en ningún momento posterior, relevando de toda responsabilidad a BilbaoTIK.

BilbaoTIK no tendrá ninguna facultad organizativa ni de dirección, ni existirá relación jurídico laboral, civil o administrativa alguna respecto a las personas que presten sus servicios para la empresa adjudicataria.

3.2. Planificación del proyecto

Una vez formalizado el contrato, y en el plazo máximo de siete (7) días naturales, se elaborará y revisará el plan de trabajo propuesto y se elaborará el plan de trabajo definitivo, que se registrará en el Acta de Inicio del contrato.

Este plan de trabajo deberá mantenerse actualizado y consensuado entre BilbaoTIK y la empresa adjudicataria.

3.3. Seguimiento y control de los trabajos

Para el seguimiento y control de los trabajos se utilizará el siguiente sistema de funcionamiento:

- La empresa adjudicataria deberá nombrar una Dirección del proyecto que será la responsable de los trabajos en todos sus aspectos. Esta persona será la encargada de convocar las reuniones de seguimiento y cuantas reuniones estime oportuno para el correcto desarrollo de los trabajos.
- La empresa adjudicataria deberá nombrar una persona responsable técnica de los trabajos que será la encargada de realizar las tareas técnicas de diseño y coordinar los recursos humanos del proyecto. Esta persona será la encargada de convocar las reuniones técnicas necesarias para la correcta definición del sistema.
- Por cada reunión de seguimiento, la empresa adjudicataria, elaborará su correspondiente acta, que deberá ser visada por las personas asistentes a la misma.
- Para el seguimiento de los trabajos será necesario entregar un informe técnico con la evolución de los trabajos. Tras la revisión técnica, la persona Responsable del Contrato y/o la Jefatura del Proyecto nombrada por BilbaoTIK, comunicará a la empresa adjudicataria el rechazo total o parcial, en su caso, de los trabajos realizados, en la medida que no respondan a lo acordado, o no superen los controles de calidad.

Inicialmente se estima un informe cada mes.

En caso de detectarse desviaciones entre la planificación y la situación real del proyecto, la empresa adjudicataria deberá emprender las acciones correctivas apropiadas, tras ser consensuadas con BilbaoTIK.

- Para dar por finalizado el proyecto y dar por cumplido el objeto del contrato, deberá validarse por BilbaoTIK el Acta de Recepción o Cierre, por el que se dará el Vº Bº a los trabajos realizados.

3.4. Condiciones generales de ejecución de los trabajos

El trabajo se desarrollará en las instalaciones de la adjudicataria. Los medios, equipos y desplazamientos necesarios del personal de la empresa adjudicataria serán a cargo de esta.

El trabajo se desarrollará siguiendo el siguiente procedimiento:

1º La adjudicataria pondrá a disposición de BilbaoTIK una cuenta de correo genérica y un teléfono en la que se atenderán las peticiones y/o consultas que se realicen.

2º El equipo técnico de la adjudicataria registrará las incidencias y todas las acciones que se vayan desarrollando para su resolución en un formato/herramienta adecuada para su gestión, sin coste adicional para BilbaoTIK.

3ª Asimismo, realizará un seguimiento de dichas acciones a medida que la incidencia se vaya gestionando y registrará el cierre una vez que BilbaoTIK dé la aceptación de su resolución y cierre.

Las incidencias serán gestionadas mediante un ANS que, como mínimo, deberá cumplir con lo siguiente:

- Las incidencias graves serán gestionadas en un máximo de 4 horas desde la recepción de los logs, notificando a BilbaoTIK telefónicamente de la existencia de la vulnerabilidad.
- Las incidencias medias y leves serán gestionadas en un máximo de 8 horas, notificando mediante la aplicación de gestión.

Toda la documentación relativa a incidencias, tareas, protocolos de actuación, etc., se debe almacenar y mantener actualizada de manera que se asegure tanto la calidad del trabajo como el traspaso de conocimiento. Asimismo, se deberá mantener un registro histórico de los cambios producidos en la documentación con una breve explicación de la causa que originó los mismos.

3.5. Documentación a entregar

La relación de entregables en este contrato será como mínimo, la siguiente: Acta de inicio, Informes mensuales del servicio y Acta de cierre.

La documentación generada durante la ejecución del contrato será propiedad exclusiva de BilbaoTIK sin que la adjudicataria pueda conservarla, ni obtener copia de esta o facilitarla a

terceros sin la expresa autorización de BilbaoTIK, que la daría en su caso previa petición formal de la adjudicataria con expresión del fin.

La documentación se entregará de forma que permita la revisión del contenido y forma necesaria, para la recepción de los distintos productos o servicios realizados y permita realizar un seguimiento adecuado del proyecto por parte de las personas responsables designadas por BilbaoTIK. La documentación se entregará en soporte electrónico de forma que BilbaoTIK pueda efectuar el mantenimiento de esta posteriormente.

La adjudicataria será responsable de mantener actualizada la documentación del proyecto a lo largo del mismo. Asimismo, deberá mantener un registro histórico de los cambios producidos en la documentación con una breve explicación de la causa que originó los mismos.

En Bilbao, a 6 de febrero de 2025

Manu Roibal
Director de Infraestructuras y Ciberseguridad
Responsable del contrato