BILBAOTIK, S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SUSCRIPCIONES DE PROOFPOINT Y CROWDSTRIKE

octubre de 2026

1.- Objeto del contrato

El Ayuntamiento de Bilbao utiliza diferentes tecnologías de seguridad para la protección de los elementos más sensibles de la red. Más en concreto, se utiliza Proofpoint como MTA de correo para el análisis y filtrado de todo el correo electrónico entrante y saliente del entorno municipal, incluyendo módulos antispam, antiphishing y antimalware, además de módulos específicos para la protección BES en toda su extensión (personas y procesos).

Por otra parte, se utiliza Crowdstrike como EDR en todos los equipos Windows, Linux y MAC de la red municipal, incluyendo equipos de escritorio de personas usuarias y servidores. En el caso del EDR se incluyen igualmente módulos específicos para la protección identidades y otros.

El objeto de este procedimiento es la adquisición de las suscripciones de Proofpoint y Crowdstrike durante un año para el volumen indicado en la tabla dentro del apartado de alcance.

2.- Alcance y descripción del contrato

En el cuadro adjunto se indican los artículos que se desean renovar:

Crowdstrike

Part Number	Descripción	Unidades
	Renovación Crowdstrike	
CS.EPPPRE.SOLN	Falcon Endpoint Protection Premium	3.400
CS.TG.STD.EU	Threat Graph Standard on EU Cloud	2.900
CS.DISC.SOLN	Discover	3.400
CS.PREVENT.SOLN	Prevent	3.400
CS.INSIGHT.SOLN	Insight	3.400
CS.TG.STD.HPSEU	Server Threat Graph Standard on EU Cloud	500
RR.HOS.ENT.ESTL	Essential Support	1
CS.FCSC.C	Falcon Cloud Security with Containers CNAPP	5
CS.CCDR.SOLN	Cloud Container Detection and Response	5
CS.TG.STD.HPSEU	Server Threat Graph Standard on EU Cloud	5
CS.FCS.PROC.SOLN	Falcon Cloud Security Proactive CNAPP	5
CS.DEVICEBP.SOLN	Falcon Device Control Bundle Promo	3.400
CS.FIREWBP.SOLN	Falcon Firewall Management Bundle Promo	3.400
CS.ITP.SOLN	Identity Threat Protection (Accounts)	5.800
CS.LEGSYS.SOLN	Falcon for Legacy Systems	2

Proofpoint

Part Number	Descripción	Unidades
	Proofpoint: Bundle P0: Email Protection (EP) + Targeted atteck Protection (TAP) + Threat Response Auto-Pull (TRAP)-Remediación Automatica + Nexus People Risk Explorer + Isolation for VAP´s	
PFPT-B-P0F-S-A	NPRE, Email Protection, TAP URL & Attachment Defense, TAP URL Iso. (VAP only), Threat Response Auto-Pull - F-Secure - SaaS	2.500
PPAO-M-LAPI-S-A	Log API Forwarding is a feature available for PoD customers to receive mail logs (filterd and sendmail) from their PoD cluster in real-time. The logs are sent in syslog format. Customers can receive these logs on common SIEM tools.	1
PP-SUP-PS	Platinum Level Support	1

Las suscripciones serán de un año, a contar desde la fecha de vencimiento de las suscripciones actuales (31/12/2026 para Crowdstrike y 15/12/2026 para Proofpoint).

Junto con las suscripciones se deberán incluir los servicios profesionales de la adjudicataria que permitan la gestión continua de la instalación. En lo referente a Crowdstrike, estos servicios deben incluir, como mínimo:

- Ayuda en la identificación precisa de incidencias y resolución de problemas detectados (compatibilidad del sensor, sistemas operativos no soportados, modo funcionamiento RFM, etc.).
- Ajuste fijo de la configuración de la plataforma y las políticas de actualización de agentes.
- Evaluación de políticas de defensa EDR atendiendo a las mejores prácticas recomendadas por el fabricante.
- Propuestas de mejoras e implementación de éstas.
- Evaluación de detecciones/incidentes y excepciones configuradas en la plataforma.
- Mejora continua de políticas incorporando nuevas funcionalidades o requerimientos.
- Servicio de monitorización y respuesta a amenazas EDR (servicio 8x5).
- Notificación de alertas relacionadas con potenciales amenazas, junto con la propuesta de respuesta.
- Resolución de dudas previo al soporte proporcionado por el fabricante.
- Alcance del servicio de monitorización amenazas en el ámbito de la identidad (SoW)
- Evaluación continua del nivel de seguridad del AD.
- Monitorización y respuesta frente a amenazas específicas en el ámbito de la identidad.
- Identificación comportamientos anómalos: IOAs (indicators of attacks) y IOCs (indicators of compromission).
- Investigación y Threat Hunting, búsqueda proactiva de amenazas de identidad.
- Análisis del uso de protocolos inseguros, eventos de seguridad relacionados con servidores críticos o utilización de cuentas de servicios en sesiones interactivas, entre otros.

Se requiere una reunión mensual de seguimiento del servicio donde la adjudicataria pueda mostrar el trabajo de los servicios profesionales realizado durante el periodo, sin menoscabo de cualquier otra reunión de urgencia que fuera necesaria.

Bilbao, a 26 de octubre de 2026

Firmado digitalmente por MANUEL ROIBAL PRIETO - 22738555L
Fecha: 2026.10.26 11:30:03 +01'00'

Manu Roibal Prieto
Director de Infraestructuras y Ciberseguridad
Responsable del contrato