



PLIEGO DE PRESCRIPCIONES TÉCNICAS

RENOVACIÓN SOFTWARE CHAINALYSIS

**TABLA DE CONTENIDOS**

1.	ANTECEDENTES Y OBJETO	1
2.	CONTENIDO DE LAS PRESTACIONES	2
3.	EJECUCIÓN DE LAS PRESTACIONES	2
4.	CONDICIONES DE SEGURIDAD	3

1. ANTECEDENTES Y OBJETO

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos del Departamento de Seguridad, en adelante DGTSI, del Gobierno Vasco tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Departamento de Seguridad.

El aumento de la delincuencia que utiliza como herramienta y objeto las tecnologías de la información deviene en el uso masivo por los delincuentes de las criptomonedas en sus transacciones.

Por esta razón la Ertzaintza, como policía integral en el ámbito de la Comunidad Autónoma de Euskadi, dispone de una herramienta que permite la investigación de ese tipo de transacciones y les proporciona:

- Rastros de evidencias auditables que puedan ser usados como prueba pericial en los tribunales.
- Geolocalización de billeteras mínimo de Bitcoin y de Ethereum.
- Integración con soluciones de análisis forense de dispositivos móviles para asistir en el análisis de artefactos relacionados con criptomonedas .
- Identificación de cambios de propiedad de criptoactivos
- Cronología de eventos relacionados con movimientos de criptomonedas

2. CONTENIDO DE LAS PRESTACIONES

El objeto de este expediente es la renovación del software de análisis de movimientos de criptoactivos, software Chainalysis licencia de investigación Network Tracing –antes conocida como Reactor–, con objeto de dar soporte tecnológico a las investigaciones que realiza la Ertzaintza.

La licencia incluye:

- Demixing: capacidad automatizada para analizar transacciones que han pasado por servicios de mezcla (mixers), facilitando su desanonimización.
- Ask Chain (BTC Only): módulo adicional especializado en la visualización detallada y contextual de relaciones en la blockchain de Bitcoin, con actualización mensual (Ask Chain - Monthly).
- Storyline: módulo complementario para la reconstrucción visual e intuitiva de flujos de fondos a nivel de transacción individual.

3. EJECUCIÓN DE LAS PRESTACIONES

La empresa adjudicataria contrae el compromiso formal, frente a la Administración, de proporcionar durante TRES AÑOS, el mantenimiento de la licencia con los correspondientes servicios asociados.

- Actualización de licencias y soporte técnico
- Soporte técnico 24x7 Platinum: incluye atención prioritaria por parte del equipo de soporte de Chainalysis vía correo electrónico, teléfono y chat, con tiempo de respuesta garantizado de 2 horas y acceso preferente a los servicios de ISP (Investigations & Special Programs).
- Nuevas actualizaciones y versiones que se generen durante la vigencia del contrato.
- Las actualizaciones deberán estar disponibles en una semana tras la liberación de la versión por parte del fabricante
- Los parches deberán estar disponibles de forma inmediata tras la liberación por parte del fabricante.

- OnGoing Case Support: 250 horas anuales de apoyo directo del equipo de investigadores de Chainalysis (ISP), para asesoramiento con objeto de realizar/optimizar un análisis de trazabilidad detallado y exhaustivo.

4. CONDICIONES DE SEGURIDAD

El adjudicatario se compromete a cumplir la política de Seguridad de la Información del Departamento de Seguridad del Gobierno Vasco y todas las normativas y procedimientos aplicables en el contexto del suministro.

El Departamento de Seguridad del Gobierno Vasco tendrá derecho a llevar a cabo auditorías para asegurarse de que el suministro se realiza de acuerdo a lo establecido en el presente pliego. Todo el material e información requerida para dichas inspecciones estará disponible sin restricciones.

La información facilitada para abordar los trabajos no se aplicará ni utilizará con una finalidad diferente a la que es objeto de este pliego ni el prestador del suministro la comunicará, ni siquiera a efectos de su conservación a terceros.

El adjudicatario y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del suministro prestado.

El adjudicatario deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Al finalizar el contrato, y una vez haya sido transferida la información al Departamento de Seguridad del Gobierno Vasco, el adjudicatario se compromete a destruir toda la información, teniendo en cuenta los distintos soportes o documentos donde esta pueda constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc. A tal efecto, una vez realizada la operación descrita, entregará una declaración por escrito al Departamento de Seguridad donde conste que así se ha realizado.