PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA LA CONTRATACIÓN DE LA RENOVACIÓN DE LICENCIA DE LA PLATAFORMA DE CANAL DE DENUNCIAS INTEGRITY LINE DE EQS PARA LA ASOCIACIÓN BC3 BASQUE CENTRE FOR CLIMATE CHANGE-KLIMA ALDAKETA IKERGAI

1. OBJETO DEL CONTRATO

El objeto del presente contrato es la renovación de licencia de la plataforma de canal de denuncias Integrity Line de EQS para la Asociación BC3 BASQUE CENTRE FOR CLIMATE CHANGE-KLIMA ALDAKETA IKERGAI.

Esta contratación es indispensable para dar cumplimiento a la obligatoriedad establecida por la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. La renovación de la solución técnica actualmente implantada responde a la necesidad de garantizar la continuidad del servicio, asegurar la integridad de los expedientes de investigación ya iniciados y mantener los protocolos de seguridad, confidencialidad y anonimato bajo los cuales se configuró el sistema original.

Los Códigos CPV asociados a este contrato son los siguientes:

- 48000000-8 (Paquetes de software y sistemas de información).
- 48219300-9 (Paquetes de software de administración).

2. CONTENIDO DE LA PRESTACIÓN DEL CONTRATO

El objeto del presente contrato consiste en la renovación de las licencias de la plataforma de canal de denuncias Integrity Line de EQS. Esta necesidad responde a la obligación legal de BC3 de mantener operativo su Sistema Interno de Información, garantizando en todo momento la continuidad técnica y la absoluta seguridad de los datos sensibles gestionados.
Para el cumplimiento de este fin, resulta imprescindible mantener el sistema actual, de modo que se aproveche la infraestructura técnica ya instalada y se preserve la configuración personalizada desarrollada específicamente para la entidad.

Asimismo, la continuidad de esta plataforma asegura la estabilidad de los protocolos internos de BC3 y elimina los riesgos críticos de seguridad y pérdida de confidencialidad que derivarían de una migración de expedientes abiertos hacia una plataforma distinta. De este modo, se garantiza un servicio eficiente, sin interrupciones y sin costes adicionales de implantación.

En consecuencia, la renovación objeto de estos pliegos deberá cumplir, como mínimo, con las siguientes especificaciones técnicas y operativas:

2.1. Configuración de usuarios e idiomas:

- Gestión de accesos: Provisión de licencias para dos usuarios con perfil habilitado de "Gestor de Casos".

- Soporte multilingüe: La plataforma deberá permitir la configuración de forma nativa de tres idiomas: euskera, castellano e inglés.

2.2. Continuidad y funcionalidades esenciales:

Dado que el Canal de Denuncias ya se halla integrado en la estructura de BC3, y con el objeto de preservar la seguridad y confidencialidad de los expedientes en trámite, la renovación de la solución técnica vigente deberá asegurar la continuidad del servicio, manteniendo íntegras las siguientes capacidades técnicas:

- Accesibilidad y anonimato: Recepción de informes de forma segura y anónima, con disponibilidad permanente, las 24 horas del día, los 7 días de la semana en cualquier idioma, permitiendo tanto la comunicación escrita como verbal mediante mensajería de voz.

- Multiplataforma: Acceso garantizado desde equipos de escritorio y dispositivos móviles.

- Personalización: Capacidad de adaptación del entorno gráfico (*look & feel*) a la identidad corporativa de la Entidad Contratante.

- Gestión de archivos y seguridad de datos: Soporte para archivos adjuntos en formato de vídeo, audio, imagen y texto, incorporando herramientas de eliminación automática de metadatos y protección proactiva frente a *malware*.

- Interlocución segura: Canal de comunicación bidireccional que permita el diálogo anónimo entre el informante y el gestor del caso mediante un buzón seguro.

- Gestión integral de expedientes: Herramientas para la tramitación completa de los casos, incluyendo mensajería directa, sistema de notificaciones, alertas de plazos y funciones de anonimización.

- Reporting y control: Generación de estadísticas personalizables, informes descargables y registro íntegro de auditoría (*Audit Logs*) para asegurar la trazabilidad de las acciones.

- Cumplimiento normativo: Cumplimiento estricto de la normativa vigente en materia de protección de datos (RGPD) y de la Directiva Europea de protección de los denunciantes (Directiva UE 2019/1937).

2.3. Requisitos de seguridad de la información:

La plataforma deberá observar los siguientes estándares de seguridad técnica:

- Cifrado: Implementación de protocolos de cifrado de alta seguridad para la protección de la información sensible.

- Auditoría y certificación: Cumplimiento verificado de la normativa de protección de datos, acreditado mediante auditoría externa de conformidad con la certificación ISAE 3000 Tipo I y Tipo II.

- Estándares internacionales: El proveedor deberá acreditar la certificación ISO/IEC 27001 o equivalente, garantizando un Sistema de Gestión de Seguridad de la Información auditado externamente.

- Ajustes de seguridad: Uso de protocolos de bloqueo automáticos para prevenir ataques de fuerza bruta y sistema de autenticación de doble factor.

- Seguridad perimetral: Empleo de *firewalls* de última generación y restricciones por dirección IP para proteger los sistemas frente a accesos no autorizados.

2.4. Actualización y soporte:

- Evolución normativa: La plataforma deberá adaptarse de manera continua a cualquier cambio o exigencia legal (local, nacional o europea) aplicable a los sistemas internos de información.

- Mantenimiento preventivo: Realización de actualizaciones periódicas para la incorporación de nuevas funcionalidades, mejoras de seguridad y ajustes normativos.

- Capacitación de nuevos usuarios: El servicio incluye la configuración inicial de cualquier nuevo usuario, así como la formación basada en su rol y orientación funcional al usuario.

- Soporte técnico integral: El servicio incluye el soporte técnico y funcional de la plataforma a través de un servicio de atención para la gestión de consultas e incidencias.

    - Se garantizará la plena operatividad de la herramienta y la resolución de dudas de uso dentro de los plazos de respuesta previstos, sin que ello suponga coste adicional alguno sobre el coste de la licencia.

    - Plazos:

        - Respuesta a correos electrónicos: El plazo máximo de respuesta será de 48 horas a contar desde la recepción efectiva del correo electrónico en la dirección habilitada a tal efecto.

        - Resolución de incidencias urgentes: El tiempo máximo de resolución será de 24 horas desde la notificación del incidente. Tendrán la consideración de urgentes aquellos fallos, errores o anomalías técnicas que impidan o comprometan la recepción, la gestión operativa, la confidencialidad o el anonimato de las comunicaciones.

        - Resolución de incidencias ordinarias y consultas generales: El plazo máximo de resolución técnica o respuesta a consultas será de 5 días hábiles, contabilizados a partir de la fecha de su notificación.