MEMORIA JUSTIFICATIVA DE LA NECESIDAD DEL GASTO

SERVICIO DE OFICINA TECNICA DE SEGURIDAD DE LA INFORMACION PARA EL CONSORCIO DE AGUAS BILBAO BIZKAIA FINANCIADO CON FONDOS PROCEDENTES DEL MECANISMO PARA LA RECUPERACIÓN Y RESILENCIA – NEXT GENERATION EU EN EL MARCO DEL COMPONENTE 5 "PRESERVACIÓN DEL LITORAL Y RECURSOS HÍDRICOS" INVERSIÓN 1 (C5.I1) DENOMINADA «MATERIALIZACIÓN DE ACTUACIONES DE DEPURACIÓN, SANEAMIENTO, EFICIENCIA, AHORRO, REUTILIZACIÓN Y SEGURIDAD DE INFRAESTRUCTURAS (DSEAR)»

1.- Objeto del Contrato.

La función principal de la Oficina Técnica de Seguridad de la Información (OTSI), es la de acompañar y proporcionar soporte en el ámbito de la Ciberseguridad. Esto abarca desde la definición de la estrategia, adaptada a las necesidades específicas del CABB, hasta la implementación de políticas, procesos y procedimientos que garanticen la continuidad y seguridad de los servicios del CABB. Además, la OTSI ayudará al CABB a cumplir con el marco legal y regulatorio en el ámbito de la ciberseguridad, como la directiva NIS2 y el Esquema Nacional de Seguridad (ENS), o cualquier otra regulación que entre en vigor durante la vigencia del contrato.

2.- Justificación de la Necesidad del Gasto

A fin de cumplir con la normativa vigente en materia de ciberseguridad tal como el Esquema Nacional de Seguridad y la Directiva Europea NIS2, el Consorcio de Aguas Bilbao Bizkaia (en adelante CABB), requiere de un apoyo especializado a nivel estratégico y técnico en esta materia, enfocado al apoyo en el desarrollo de políticas y normativas internas, gestión de riesgos, coordinación de proyectos, formación y control del cumplimiento de la regulación vigente.

Necesitamos la OTSI para realizar actividades vinculadas a la seguridad proactiva, en concreto:

- Implantación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI), realizando la revisión y actualización del análisis de riesgos, incluido el inventariado de activos, la definición y elaboración del modelo de dependencias, el diseño, obtención y análisis de resultados de encuestas para valoración de activos, la identificación y valoración de las amenazas, la identificación y valoración de salvaguardas, la estimación del riesgo, la proyección del riesgo etc.
- Elaboración o revisión de normas, procedimientos, protocolos, instrucciones técnicas y guías de seguridad de la información (técnicas y no técnicas).
- Desarrollo y seguimiento del cuadro de mando de indicadores.

El marco de trabajo de referencia será la norma ISO 27001 y la ISO 20000 y subsiguientes, así como otras metodologías en el ámbito de la seguridad de la información ampliamente reconocidas (Leet, ENS, NIST, SANS, COBIT, etc.).

- Asesoramiento experto en materia regulatoria en el ámbito de la seguridad de la información y la ciberseguridad, en particular en las leyes vigentes en los siguientes ámbitos:
    - Esquema Nacional de Seguridad
    - Esquema Nacional de Interoperabilidad

    - Protección de Infraestructuras Críticas y Servicios Esenciales
    - Protección de Datos de Carácter Personal
    - Firma electrónica
    - NIS – Normativa europea de seguridad de las redes y sistemas de información.
- Apoyo a la continuidad del negocio, realizando al menos las siguientes tareas
    - Elaboración del Análisis de Impacto en el Negocio (BIA).
    - Revisión de los Planes de Recuperación ante Desastres y pruebas asociadas, para la detección de deficiencias y elaboración de propuestas de mejora e identificación de oportunidades.
- Consultoría y asesoramiento especializado en cualquier aspecto relacionado con la seguridad de la información y la ciberseguridad, entre otros y sin que se trate de una relación exhaustiva, los siguientes:
    - Seguridad Perimetral (WAF, NGF, IDS/IPS, etc.)
    - Seguridad en el puesto de trabajo (end-point).
    - Seguridad en dispositivos móviles.
    - Arquitecturas de seguridad y segmentación de redes.
    - Seguridad en los protocolos de comunicación.
    - Bastionado y hardening de sistemas, servidores y servicios.
    - Seguridad en la nube (Saas, PaaS, IaaS, etc.).
    - Gestión de logs y correlación de eventos de seguridad.
    - Malware.
    - Mecanismos de autorización, acceso y autenticación.
    - Desarrollo seguro de software.
    - Acreditación de sistemas.
- Elaboración y programación de informes estadísticos y de detalle sobre las herramientas de seguridad disponibles por CABB (Antivirus, Antispam, Gestor de navegación segura, etc.).
- Soporte a las actividades de divulgación y concienciación en materia de seguridad de la información, realizando al menos las siguientes tareas
    - Elaboración de propuestas formativas (Módulos formativos, Newsletters, Guías, píldoras, etc.).
    - Generación de contenidos divulgativos relacionados con la prevención y respuesta a incidentes de seguridad.
    - Impartición de seminarios y formación relacionada con la seguridad TIC al personal del CABB.

El importe estimado es de 450.000 euros, IVA excluido, por lo que se considera licitar por concurso abierto.

Bilbao,20 de marzo de 2025
El Subdirector del Departamento de Informática

Fdo: José Luis Unzueta

Bilbao, 1 de abril de 2025
Responsable de Proyectos de Informática

Fdo: Marian Mena