JUSTIFICACIÓN DE LA NO DISPOSICIÓN DE MEDIOS

SERVICIO DE CENTRO DE OPERACIONES 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

El objeto de los trabajos a realizar por el adjudicatario en el ámbito del presente contrato será la prestación de servicios de seguridad de la información y ciberseguridad, como soporte al área de Seguridad Lógica del CABB. Para ello, se contará con un Centro de Operaciones de Seguridad (en adelante, SOC) que será el encargado de prestar dichos servicios.
De manera general, el SOC prestará un servicio permanente (24x7) de monitorización, supervisión, detección y gestión de incidentes de seguridad, enfocándose en la seguridad preventiva y reactiva.
El SOC prestará, como mínimo, los siguientes servicios:

Ciberinteligencia

El adjudicatario proveerá un servicio de inteligencia digital para la recolección de datos e información a partir de diferentes fuentes, realizando su investigación y análisis de los resultados con el fin de detectar precozmente posibles amenazas online que puedan afectar al CABB, incluyendo, como mínimo, las siguientes:

- Fugas de información
- Protección de activos
- Amenazas Avanzadas Persistentes (APTs)
- Movimientos sociales y hacktivistas
- Protección VIP
- Protección de marca, presencia y reputación online

Monitorización de la seguridad

El adjudicatario supervisará permanentemente el estado de la infraestructura tecnológica de CABB, generando las alertas correspondientes en caso de eventos que puedan afectar la seguridad de la compañía. Las principales tareas a realizar son la monitorización y supervisión proactiva de los eventos de seguridad a través de un correlador de eventos de seguridad (SIEM). Se realizará el procesamiento y correlación de los eventos recolectados en tiempo real para la detección anticipada de sucesos relevantes que puedan ser indicativos de un ataque, así como el análisis y verificación para desestimar falsos positivos y la elaboración de indicadores de cumplimiento y desempeño.

Gestión de incidentes de seguridad

Una vez se detecte un incidente a través del servicio de monitorización, o bien este sea comunicado por alguno de los canales establecidos, el SOC procederá a la gestión completa del incidente, realizando, al menos, las siguientes actividades: registrar, clasificar, valorar, priorizar y escalar los incidentes de seguridad detectados a través del servicio de monitorización; emitir las alertas oportunas ante eventos de seguridad; realizar la notificación y documentación de los incidentes de seguridad; adoptar medidas de contención para

los incidentes de seguridad; investigar los incidentes de seguridad, localizando y recolectando evidencias; realizar el análisis de código malicioso; investigación forense; elaborar el informe de cierre del incidente, así como el informe post-incidente, incluyendo lecciones aprendidas y propuestas de planes de acción para prevenir la reproducción futura de incidentes similares o mejorar los mecanismos de respuesta y gestión de incidentes.
Entre otras tareas, el adjudicatario se encargará de probar los procedimientos de respuesta ante incidentes y preparará ciberejercicios para que se realicen por parte de la organización. También deberá revisar periódicamente los procedimientos, manuales y herramientas definidos para la gestión de incidentes de seguridad.

Servicio de Auditorías de Seguridad y Análisis de Vulnerabilidades

El objetivo de este servicio es identificar vulnerabilidades o fallos de seguridad en las redes y sistemas de información de CABB frente a ataques externos e internos, cubriendo tanto los sistemas de información (IT) como los sistemas industriales (OT). Para ello, se realizarán las siguientes tareas:

- Auditoría de seguridad perimetral
- Auditoría interna
- Análisis de vulnerabilidades
- Test de seguridad (hacking ético)
- Auditoría de código

2. Justificación de no disposición de medios

El Consorcio carece de recursos internos para atender dichos servicios.

Bilbao, a 20 de marzo de 2025.

El Subdirector de Informática,

Jose Luis Unzueta Portilla