PLIEGO DE CONDICIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DE UN SISTEMA DE CIBERSEGURIDAD BASADO EN INTELIGENCIA ARTIFICIAL PARA EL MUSEO GUGGENHEIM BILBAO

1. OBJETO DEL CONTRATO

El objeto del contrato es la instalación del equipamiento necesario para disponer de un sistema de ciberseguridad basado en inteligencia artificial y los servicios de operación (SOC) asociados al mismo, para la Fundación del Museo Guggenheim Bilbao (en adelante, la Fundación)

2. ALCANCE DEL CONTRATO

2.1 Situación actual

En la actualidad la Fundación dispone de sistemas de seguridad basados en firewalls y antimalwares XDR en los puestos de usuario y servidores.

2.2 Necesidades

La Fundación busca un sistema de ciberseguridad avanzado que permita analizar y saber qué información está circulando por la red. Estará basado en inteligencia artificial (IA) que utilice algoritmos de aprendizaje automático y técnicas avanzadas para proteger y fortalecer la seguridad de los sistemas y las redes de datos contra amenazas. Este sistema aprovechará las capacidades de la IA para analizar y detectar patrones de comportamiento, identificar anomalías y amenazas potenciales, y tomar medidas de manera automatizada o asistida por humanos, para mitigar los riesgos de las amenazas de seguridad. También son necesarios los servicios de operación SOC prestados por una empresa experta en seguridad y en el sistema elegido.

2.3 Características del sistema a implantar

El sistema de ciberseguridad deberá disponer de las siguientes características:

1. **Detección de amenazas avanzadas**: Análisis de grandes volúmenes de datos y detección de patrones inusuales o comportamientos maliciosos, tal y como ocurre en las fugas de información.
2. **Análisis de comportamiento en tiempo real**: Monitorización del comportamiento de los usuarios, aplicaciones y sistemas.
3. **Respuesta automatizada**: Activación de medidas inmediatas y automatizadas para contener y mitigar la amenaza sin intervención humana.
4. **Adaptabilidad y aprendizaje continuo**: Aprendizaje de los algoritmos de IA para aprender y adaptarse a nuevas amenazas y patrones a medida que evolucionan.
5. **Reducción de falsos positivos**: Reducción de detecciones erróneas.
6. **Identificación de vulnerabilidades**: Análisis continuo para proporcionar recomendaciones.

2.4 Alcance de áreas protegidas

El sistema de ciberseguridad debe proteger las siguientes áreas de la Fundación:

1. RED DE ÁREA LOCAL. El sistema, en su actuación dentro de la red de área local, debe:

   a. Mitigar ataques de malware que se propagan lateralmente por la red.
   b. Identificar dispositivos comprometidos que generan tráfico sospechoso.
   c. Responder a conexiones maliciosas con servidores de comando y control.
   d. Aprender el estado normal del tráfico y comportamiento de la red.
   e. Detectar rápidamente desviaciones o comportamientos anómalos.
   f. Aislar dispositivos comprometidos o limitación de su tráfico malicioso.
   g. Operar en los modos: **Pasivo** (solo monitoreo y alertas), **Activo supervisado** (respuestas automáticas sujetas a aprobación) y **totalmente autónomo** (acciones inmediatas sin intervención humana).
   h. Realizar análisis forenses para entender el origen de un ataque, los vectores utilizados y las vulnerabilidades.

Notas importantes:
- La protección en la red local tiene que incluir todas las VLAN de usuarios y servidores, DMZ, I-oT, VPN, etc.
- El número de direcciones IP a monitorizar será de un mínimo de 300 si bien la oferta deberá incluir la posibilidad de monitorización de al menos hasta 330.

2. CORREO ELECTRÓNICO. La Fundación utiliza Microsoft 365 como herramienta de correo corporativo. La protección ofrecida por el sistema de ciberseguridad deberá:

   a. Neutralizar amenazas avanzadas tales como: *phishing, malware y ransomware*.
   b. Aprender el patrón habitual de comunicación de cada usuario que tenga en cuenta el estilo de escritura, las horas frecuentes de envío, las conexiones habituales, etc.
   c. Detectar desviaciones sutiles de sintaxis, tales como pequeños cambios en el dominio (ejemplo: example.com frente a examp1e.com).
   d. Funcionar sin depender exclusivamente de reglas, listas negras o firmas conocidas, permitiendo detectar amenazas nunca vistas anteriormente.
   e. Poner en cuarentena los correos sospechosos y redirigirlos para revisión por parte del equipo de seguridad.
   f. Etiquetar correos con advertencias visibles para el usuario.
   g. Evaluar contexto y contenido para minimizar falsos positivos.
   h. Analizar contenido y contexto de cada correo: (i) análisis de enlaces (URLs), (ii) adjuntos maliciosos, (iii) estilo de redacción con lenguaje inusual o mensajes fuera de contexto en relación con el remitente esperado.
   i. Ver al completo el flujo de Email con atención a dominios nuevos en la red de comunicación o usuarios que reciben mensajes no esperados desde ubicaciones sospechosas.

Nota importante:
- El número aproximado de mensajes recibidos durante 2024 fue de 550.000 y de mensajes enviados de 300.000.

2.5 Servicio externo de acompañamiento

El sistema se explotará en modo de Centro de Operaciones de Seguridad (SOC). La empresa contratista realizará tareas de monitorización además de ayudar y asesorar al personal de la subdirección de Tecnologías de la Información. Este servicio se realizará en todo caso atendiendo a las indicaciones de la Fundación que dispondrá de una consola totalmente operativa desde la que pueda gestionar el sistema y consultar toda la información monitorizada. Los servicios SOC se prestarán en modo 24x7x365. En la oferta, deberá detallarse, en su caso, la propuesta de subcontratación de otras empresas.

2.6 Implantación, garantía y mantenimiento

Se deberá presentar un plan de implantación del sistema con un calendario de trabajo detallado, la relación de personal técnico asignado y la documentación entregada.

La garantía, el soporte y el mantenimiento del sistema descrito en este Pliego se deberá proporcionar durante un periodo de **duración del contrato y sus prórrogas en su caso**. Durante ese periodo se incluirá el **suministro e instalación** de todos los parches y todas las nuevas versiones de software que vayan apareciendo.

Se solicitan los siguientes niveles de servicio para el servicio de mantenimiento:

-El **servicio de atención** deberá estar disponible para recogida de avisos de avería durante las 24 horas del día y los 7 días de la semana, con atención telefónica personal durante la jornada laboral.

-El **tiempo de respuesta** ante una incidencia dependerá de la criticidad de la avería. Se considerarán los siguientes valores de referencia para el servicio solicitado:

Tiempo de respuesta al aviso:
- Será de 8 horas en horario laboral
- Primera hora del primer día siguiente al aviso, para avisos fuera del horario laboral

Tiempo de presencia "in situ":
- Será de 8 horas en horario laboral para averías graves
- Primera hora del día siguiente al aviso para el resto de las averías

2.7 Formación y transferencia de conocimiento

Durante toda la implantación se realizará una formación práctica y una transferencia de conocimiento a los gestores de la Fundación para ser autónomos en la administración y gestión del sistema.

Se debe incluir el acceso a los exámenes de certificación oficial del fabricante para una persona y el material formativo necesario.