PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DE LOS SERVICIOS DE UNA OFICINA TÉCNICA DE SEGURIDAD PARA DAR APOYO A LA AGENCIA DE RESIDUOS DE CATALUÑA (ARC)

1.- OBJETO DEL PROCEDIMIENTO ABIERTO

El objeto de la presente licitación es la de proporcionar los datos necesarios para la contratación de los servicios de una oficina técnica de seguridad para la ARC.

La contratación se realizará mediante un procedimiento abierto y tendrá como objeto el servicio de una oficina técnica de seguridad.

2.- PLAZO DE ENTREGA Y DURACIÓN DEL CONTRATO

El plazo de ejecución se desglosa de la siguiente manera: el plazo de inicio del servicio será de 2 semanas a partir de la formalización de la adjudicación y firma del contrato.

La duración del contrato será de un año, y no se iniciará antes del 1 de enero del 2026 y finalizará el 31 de diciembre de 2026.

Se prevé que se pueda prorrogar durante 4 años, con 4 prórrogas de un año, así la duración total máxima del contrato podrá ser, en caso de ejecutarse todas las prórrogas, de 5 años.

Si en algún momento la Agencia de Ciberseguridad de Cataluña (ACC en adelante) nos comunica que ya puede asumir todas las funciones descritas en este pliego de Prescripciones Técnicas, se procedería a no renovar la siguiente prórroga.

3.- JUSTIFICACIÓN DE LA NECESIDAD E IDONEIDAD DEL CONTRATO

La contratación de una oficina técnica de seguridad, incluyendo la figura CISO (“Chief Information Security Officer”), responde a la necesidad de asegurar el cumplimiento normativo y la protección de los sistemas de información, infraestructuras esenciales y activos digitales de la organización. El aumento de las ciberamenazas y la creciente regulación en materia de seguridad y protección de datos hacen imprescindible contar con especialistas que puedan diseñar, implementar y supervisar estrategias de seguridad de manera continua y eficiente, que garanticen la protección de los recursos tecnológicos y la confidencialidad, integridad y disponibilidad de la información, siempre de forma coordinada con la ACC.

Otros aspectos relevantes que justifican su contratación son la aportación de conocimiento especializado, flexibilidad y capacidad de adaptación a nuevas amenazas. También contribuye a la detección y respuesta rápida ante incidentes, minimizando el impacto de posibles vulnerabilidades. Asimismo, facilita la implementación de medidas proactivas para la seguridad de la información y la protección de infraestructuras críticas. En conjunto, esta contratación refuerza la resiliencia de la organización y garantiza un entorno tecnológico seguro y eficiente.

4.- DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

La ARC ya dispone de un conjunto de medidas de seguridad perimetral para proteger sus infraestructuras, las cuales son objeto de este procedimiento abierto. Actualmente, la ARC cuenta con:

- EDR Implementado en estaciones de trabajo y servidores para la detección y respuesta ante amenazas en los endpoints. El centro de control y monitorización pertenece a la ACC, y así tiene que continuar.
- Firewall: Utilizado para la protección perimetral de la red, controlando el tráfico de entrada y salida.
- WAF: Desplegado para proteger las plataformas web de la ARC contra ataques específicos a aplicaciones web.
- Tanto el Firewall como el WAF están alojados actualmente en nuestro Centro de Procesamiento de Datos (CPD).
- Autenticación de doble factor: Requerida para todos los usuarios que acceden a las infraestructuras, añadiendo una capa extra de seguridad.

La ARC está comprometida con el cumplimiento del Esquema Nacional de Seguridad (ENTE) en su categoría media. Eso implica, que se tienen que implementar un conjunto de medidas de seguridad específicas para proteger sus sistemas de información y garantizar la confidencialidad, integridad y disponibilidad de los datos.

La incorporación de un CISO (Chief Information Security Officer) reforzará estas medidas de seguridad existentes y permitirá implementar nuevas estrategias y tecnologías para alcanzar un nivel de seguridad óptimo. El/La CISO será responsable de liderar la gestión de la seguridad de la información, asegurando la protección de los activos de la ARC y la conformidad con las normativas aplicables, siempre con la coordinación y bajo las directrices de la ACC.

5.- REQUISITOS TÉCNICOS DE OBLIGADO CUMPLIMIENTO

5.1. Requisitos del servicio

Los servicios que se están solicitando tienen que cubrir tanto el ámbito de la seguridad de la información como el cumplimiento normativo durante todo el periodo de vigencia del contrato.

La Oficina Técnica de Seguridad estará integrada por varios servicios, cada uno con un ámbito de actuación, tareas y recursos específicos, tal como se detalla a continuación.

5.1.1. **Servicio de Gestión y Administración de la Seguridad**:

a. Tendrá que incluir un perfil que realizará las funciones de CISO (Chief Information Security Officer): Que tendrá que realizar la definición y dirección estratégica de la seguridad, a partir de las directrices de la ACC, realizar la definición de políticas y supervisión de las medidas de protección.
b. Análisis y gestión de riesgos de seguridad: Identificación de amenazas, impactos y medidas de mitigación.
c. Creación y gestión de planes directores de seguridad: Desarrollo y manteniendo durante todo el servicio una hoja de ruta para la mejora continua de la seguridad de la información.
d. Definir los indicadores de seguridad (KPI/KRI), por la medición y control del rendimiento de las medidas de seguridad.
e. Colaborar y dar apoyo a la ACC en la definición e implementación de medidas de seguridad, auditoría, respuesta a incidentes de seguridad y otras acciones que puedan ser necesarias para mejorar la seguridad y cumplimiento normativo de la ARC.
f. Elaboración de planes de contingencia y respuesta a incidentes: Definición de procedimientos para minimizar el impacto de ataques o fallos alineado con el Esquema Nacional de Seguridad (ENTE).
g. Auditorías de seguridad, con objetivo de realizar la verificación de controles establecidos, realizando revisiones periódicas de los planes, directrices y procesos de seguridad establecidos.
h. Gestión de la continuidad del negocio (BCP- Business Continuity Plan), diseñando las medidas necesarias para garantizar la disponibilidad de los servicios esenciales.

5.1.2 **Servicio de soporte al Cumplimiento Normativo**:

a. Definir, proponer y ejecutar el plan de adecuación al Esquema Nacional de Seguridad (ENTE), y proporcionar el apoyo técnico necesario para realizar la adecuación de la ARC.
b. Programar y ejecutar acciones de concienciación y formación para empleados: Elaboración de documentación para usuarios sobre la seguridad digital y Esquema Nacional de Seguridad.
c. Simulación de phishing e ingeniería social: Campañas para detectar y reducir el riesgo de ataques basados en engaños, para evaluar el nivel de sensibilización de los empleados de la ARC.

5.1.3 Servicio de Operación de la Seguridad:

a. Dar apoyo a la supervisión de los sistemas de seguridad de la ARC para la monitorización y detección de amenazas, integrando los datos e inteligencia proporcionadas por la ACC para una detección y respuesta más efectiva de incidentes.
b. Evaluación de vulnerabilidades para mejorar la protección de los sistemas y la realización de tests de penetración (pentesting).
c. Apoyo a la gestión de vulnerabilidades, protección de sistemas y aplicación de medidas para corregir riesgos de seguridad.
d. Apoyo pericial informático forense en casos de delitos informáticos, fraude, robo de datos, disputas legales que involucren evidencias digitales, y cualquier otro caso en que la información digital sea relevante para la resolución del litigio.
e. Colaborar y dar apoyo a la ACC en la implantación de medidas de seguridad, auditoría, respuesta a incidentes de seguridad y otras acciones que puedan ser necesarias para mejorar la seguridad y cumplimiento normativo de la ARC.
f. Pruebas de recuperación y simulacros: Ejercicios para comprobar la eficacia de los planes de respuesta ante incidentes.

5.1.4 Otros servicios:

a. Se tiene que incluir un **Servicio de Gestión y Apoyo a la Seguridad,** que permita gestionar y documentar los incidentes de seguridad, según el que establece la Guía CCN-STIC 817, basado en una plataforma online, ofreciendo a la ARC acceso continuo e información en tiempo real a la información, estado del incidente, acciones realizadas, desde cualquier ubicación.
b. Se tiene que incluir un **Servicio de Vigilancia de Seguridad,** basado en una plataforma online, que permita la monitorización del entorno digital de la ARC (Vigilancia Digital), ofreciendo a la ARC acceso continuo y en tiempo real a la información desde cualquier ubicación.
c. Se tiene que incluir un **Servicio de Monitorización** de los indicadores de seguridad**,** que permita la actualización automática y visualización de los KPI/KRI de seguridad establecidos, ofreciendo a la ARC acceso continuo e información en tiempo real a la información desde cualquier ubicación.

Se requiere la presentación de un plan de trabajo, detallado que especifique las tareas a realizar durante el primer año. Para los años sucesivos, el licitador tendrá que elaborar y presentar un nuevo plan de trabajo un mes antes de la finalización del periodo en curso, el cual tendrá que ser validado y aprobado por la ARC. Estos planes de trabajo tienen que cubrir los servicios descritos en este pliego técnico y prever un esfuerzo anual de entre 750 y 800 horas, incluyendo una reserva mínima de 50 horas para la gestión de incidentes de seguridad o solicitudes no planificadas.

5.2. Perfiles profesionales mínimos requeridos

El licitador tendrá que disponer y asignar a este servicio de un equipo de trabajo que cumpla con los siguientes perfiles profesionales mínimos, con el objetivo de garantizar la correcta ejecución de los servicios objeto de este pliego:

a. Experto en seguridad de la información:
   - Titulación universitaria en ingeniería informática, telecomunicaciones o similar.
   - Experiencia mínima de 5 años en gestión de la seguridad de la información.

b. Especialista en Esquema Nacional de Seguridad (ENTE) y protección de datos:
   - Titulación universitaria en Derecho e inscripción vigente como abogado/a a un Colegio de Abogados.
   - Conocimientos avanzados en RGPD y LOPDGDD y Esquema Nacional de Seguridad (ENTE).

c. Analista de seguridad:
   - Titulación universitaria o de Técnico Superior en Informática, Ciberseguridad o áreas relacionadas.
   - Experiencia mínima de 3 años en el uso de herramientas de ciberseguridad, análisis de vulnerabilidades y pruebas de intrusión.

d. Perito Judicial Informático Forense:
   - Titulación universitaria o de Técnico Superior en Informática, Ciberseguridad o áreas relacionadas.
   - Experiencia mínima de 3 años en tareas de perito informático Forense.

5.3. Otras consideraciones

5.3.1. Conformidad con el Esquema Nacional de Seguridad (ENTE)

La empresa adjudicataria tendrá que acreditar la conformidad con el Esquema Nacional de Seguridad (ENTE) en categoría media para todos los servicios incluidos en este pliego. A

tal efecto, se tendrá que adjuntar a la memoria técnica el correspondiente certificado emitido por la entidad certificadora en lo que se especifiquen estos servicios dentro de su alcance.

5.3.2. Licencias de software

La oferta presentada tiene que incluir las licencias necesarias para una plataforma en línea unificada que permita cubrir todos los requisitos indicados en los servicios detallados en el apartado 'Otros servicios'.

5.3.3. Lugar de prestación del servicio

Este servicio se prestará combinando tareas presenciales y remotas (no presenciales). Las tareas presenciales se realizarán en:

- La sede de la ARC, en la Avenida de la zona Franca, 107- 08038 Barcelona
- En el CPD actual ubicado en la Calle Doctor Roux, 80 -08036 Barcelona

Añadir que la ARC está en pleno proceso de transformación al Modelo Corporativo de la Generalitat y está previsto que, entre otras medidas, a lo largo del 2025 o principios del 2026 el actual CPD ubicado en el C/Doctor Roux 80 desaparezca y se mueva a la nube en un entorno Corporativo.

El prestatario estará obligado a utilizar sus propios equipos informáticos de usuario: PC, ordenador portátil o cualquier otro dispositivo de informática móvil que considere necesario. En ningún caso la ARC proveerá de los dispositivos informáticos ni telefónicos al proveedor.

5.3.4. Horario

Las tareas establecidas en este servicio se realizarán dentro del horario laboral de la ARC a menos que las intervenciones planificadas interfieran en el buen funcionamiento de los sistemas informáticos. Si es este el caso, se podrá planificar las intervenciones fuera del horario laboral siempre con la conformidad previa de la ARC.

En caso de incidente de seguridad, habrá que proporcionar un apoyo continuo en las operaciones de seguridad, con actuaciones fuera del horario laboral, si es necesario para mitigar el incidente.

Todas las actuaciones fuera del horario laboral, en caso de que sean necesarias, estarán incluidas dentro del alcance de la propuesta.

5.3.5. Certificaciones

En la presentación de la oferta se tendrán que aportar copias de las certificaciones, títulos y colegiación del personal asignado al servicio. Los certificados aportados tendrán que estar vigentes a la fecha de presentación de las ofertas.

6.- PROPUESTA TÉCNICA

Los licitadores pueden adjuntar a su oferta toda la información complementaria que consideren de interés. Sin embargo, tendrán que presentar unos contenidos mínimos y estar obligatoriamente estructurada de la forma que se indica en los anexos adjuntos:

- Anexo 1: modelo de propuesta para la documentación relativa a los criterios de juicio de valor.
- Anexo 2: modelo de propuesta para la documentación relativa a los criterios ponderables de forma automática.

7.- CONFIDENCIALIDAD

Toda la información facilitada por la ARC que la empresa contratada tenga que utilizar por motivos profesionales, se considerará estrictamente confidencial y así será tratada.

8.- PRESUPUESTO

El precio se ha determinado a partir de los precios de mercado del hardware, software y apoyo, objetos del presente contrato una vez consultadas empresas especializadas del sector. A partir de este cálculo, determinamos que el precio, a tanto alzado, de esta licitación será de 65.000 € + 13.650 € que corresponden al 21% del IVA.

9.- ENTREGA Y PAGO

El pago se hará mensualmente, previa presentación de la factura correspondiente, contra la certificación acreditativa por parte del jefe del Departamento de Tecnologías de la Información de la correcta realización del suministro y de las tareas efectuadas.

Jefe del Departamento de
Tecnologías de la Información

Agència de Residus de Catalunya

ANEXO 1

MODELO DE PROPUESTA PARA LA DOCUMENTACIÓN RELATIVA A LOS CRITERIOS DE JUICIO DE VALOR PARA EL SUMINISTRO DE LOS SERVICIOS DE OFICINA TÉCNICA DE SEGURIDAD PARA DAR APOYO A LA AGENCIA DE RESIDUOS DE CATALUÑA (ARC)

PUNTUACIÓN TOTAL: 30 PUNTOS

- **Descripción de los servicios ofrecidos en el apartado "5.1.4 Otros servicios" (puntuación máxima: 15 puntos).**
  De esta descripción se valorará el detalle de los servicios ofrecidos para dar respuesta a los requerimientos del apartado "5.1.4 Otros servicios", idoneidad y adecuación con las necesidades de la ARC, integración con el resto de servicios de la Oficina Técnica de Seguridad y nivel de cumplimiento normativo. Esta descripción no tendrá que superar las 6 páginas en formato A4, utilizando la tipografía Arial 10.

- **Propuesta de planificación del servicio para el primer año. (puntuación máxima: 8 puntos).**
  De esta propuesta de planificación se valorará su adecuación a los requisitos técnicos, la idoneidad y calidad de las tareas, la capacidad de gestión, ejecución y seguimiento, la innovación y la claridad de la presentación. Esta planificación se tiene que presentar en una única página en formato A4.

- **Modelo de relación y gestión del proyecto (puntuación máxima: 7 puntos).**
  En este modelo de relación y gestión del proyecto, se valorará la claridad, la facilidad de seguimiento, la facilidad de comunicación, la claridad en la definición de responsabilidades, la adaptabilidad a cambios, y la capacidad para resolver problemas y cumplir los objetivos definidos. Esta descripción no tendrá que superar las 10 páginas en formato A4, utilizando la tipografía Arial 10.

ANEXO 2

MODELO DE PROPUESTA PARA LA DOCUMENTACIÓN RELATIVA A LOS CRITERIOS PONDERABLES AUTOMÁTICAMENTE DEL LOTE 1 PARA EL SUMINISTRO DE LOS SERVICIOS DE OFICINA TÉCNICA DE SEGURIDAD PARA DAR APOYO A LA AGENCIA DE RESIDUOS DE CATALUÑA (ARC)

PUNTUACIÓN TOTAL: 70 PUNTOS

- **Oferta económica (puntuación máxima: 40 puntos)**

La fórmula de cálculo de este criterio será la siguiente:

$$P_v = \left[1 - \left(\frac{O_v - Om}{IL}\right) \times \left(\frac{1}{VP}\right)\right] \times P$$

Pv = Puntuación de la oferta a valorar P = Puntos criterio económico (30 puntos)

Olmo = Oferta mejor Ov = Ofrecida a valorar

IL = Importe de licitación VP = Valor de ponderación

Vistas las características críticas de este proyecto, el VP será igual en 4

- **Acreditar la conformidad con el Esquema Nacional de Seguridad (ENTE) en categoría alta (puntuación máxima: 10 puntos)**

Acreditar la conformidad con el Esquema Nacional de Seguridad (ENTE) en categoría alta para todos los servicios incluidos en este pliego. (10 puntos)

- **Disponer de certificaciones técnicas (puntuación máxima: 20 puntos)**

Se concederán puntos adicionales por las certificaciones técnicas reconocidas en el ámbito de la ciberseguridad, que demuestren un alto nivel de conocimientos y habilidades en las áreas pertinentes de los perfiles profesionales asignados a este servicio.

- 1 perfil con título de Máster Universitario Oficial en Ciberseguridad. (5 puntos).
- 1 perfil con el certificado de Perito Judicial Informático Forense colegiado (5 puntos).
- 1 perfil con el certificado Certified Ethical Hacker (CEH) (5 puntos).
- 1 perfil con el certificado Offensive Security Certified Profesional (OSCP) (5 puntos).

No se otorgarán puntos para presentar más de un perfil con la misma certificación.