ATM Àrea de Barcelona
Autoritat del Transport Metropolità

Pliego de Prescripciones Técnicas para la contratación mediante procedimiento abierto sujeto a regulación armonizada de los servicios de:

Fase III Externalización CISO

(Exp. C-25/2025)

Diciembre 2025

Balmes, 49, 6a planta, 08007 Barcelona
Autoritat del Transport Metropolità. NIF: P-5890049-I

ÍNDICE

1. Prescripciones generales 3
2. Contexto 3
3. Objeto del contrato 5
4. Actividades y funciones de la empresa adjudicataria 6
4.1. Rol de CISO externalizado 6
4.2. Rol de experto en Gobernanza, Riesgo y Cumplimiento (GRC) 7
4.3. Sistema de monitorización y gestión de acontecimientos e información de seguridad 8
4.4. Servicio de gestión y configuración de seguridad y respuesta ante incidentes 8
5. Finalidades y objetivos que lograr ..... **Error! No s'ha definit el marcador.**
6. Requerimientos técnicos generales obligatorios de la prestación y/o rendimiento o exigencias funcionales de la prestación 11
7. Formas de seguimiento y control de la ejecución de las condiciones 12
8. Calendario de trabajo y duración del Contrato 14
9. Condiciones generales de ejecución y ciberseguridad 14
9.1. Principios básicos 14
9.2. Marc de cumplimiento normativo 15
9.3. Datos de carácter personal 15
9.4. Esquema Nacional de Seguridad (ENS) 16
9.5. Seguimiento 17
10. Documentación técnica que tienen que aportar las empresas licitadoras 17

1. Prescripciones generales

Este pliego de prescripciones técnicas tiene por objeto determinar el contenido y el alcance de las tareas que tendrá que desarrollar la empresa contratista en estos servicios y los requisitos que tiene que cumplir para ser adjudicataria, así como fijar las condiciones técnicas a las cuales tendrán que ajustar los trabajos a realizar.

Con este objetivo, se describen los trabajos a realizar y su desarrollo y se relacionan las materias que tienen que servir de base para licitar y garantizar la calidad de las propuestas.

Así mismo, se describen las características y contenido de las ofertas a presentar y los criterios que servirán de base, tanto para la adjudicación de los trabajos como para que estos sean aceptados por la dirección de la asistencia técnica.

La dirección de los servicios y su aprobación dependerán del Área de Sistemas e Innovación de la Autoritat del Transport Metropolità, Consorcio para la coordinación del sistema metropolitano de transporte público del Área de Barcelona (ATM, de ahora en adelante).

Con la presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

2. Contexto

La Autoritat del Transport Metropolità del área de Barcelona (en adelante ATM) es un consorcio interadministrativo de carácter voluntario, creado el 1997. Actualmente, las administraciones consorciadas son la Generalitat de Cataluña (51%) y administraciones locales (49%), compuestas por el Ayuntamiento de Barcelona, el Área Metropolitana de Barcelona (anteriormente denominada Entidad Metropolitana del Transporte) y la Asociación de Municipios para la Movilidad y el Transporte Urbano (AMTU). A dicho consorcio se pueden adherir todas las administraciones titulares de servicios públicos de transporte colectivo que pertenezcan al ámbito formado por las comarcas del Alt Penedès, Anoia, el Bages, el Baix Llobregat, el Barcelonès, el Berguedà, el Garraf, el Maresme, Osona, el Vallès Occidental y el Vallès Oriental. Además, la Administración General del Estado está presente en los órganos de gobierno de la ATM en calidad de observador.

El Área de Sistemas e Innovación tiene encomendadas, entre otras, la gestión de las políticas de seguridad informática y de protección de datos, la de los sistemas de seguridad en red y la de los sistemas corporativos de autenticación de usuarios. Esta Area administra una infraestructura de comunicaciones y servidores que proporciona el apoyo sobre el cual se implementan las aplicaciones corporativas, se distribuye la información de sus servicios

y se prestan los servicios telemáticos a la ciudadanía. En consonancia con el principio básico de "Líneas de defensa" establecido en el Real Decreto 311/2022 del 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENS), para asegurar estas comunicaciones, hay que orientar la estrategia de seguridad hacia una solución de arquitectura multicapa, consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de que los sistemas de información se vean comprometidos y minimizar el impacto si la situación de riesgo se llega a materializar.

Por otro lado, la nueva Directiva europea de Ciberseguridad, NIS2, aprobada en 2023, es aplicable a todos los Estados miembros a partir de 2025 y forma parte del pilar central de la resiliencia digital de Europa. Es una directiva de seguridad y resiliencia, no solo tecnológica: afecta procesos, gobernanza, cadena de suministro y responsabilidades de dirección.

La ATM dispone de un rol de CISO (“Oficial de Seguridad de la Información”) contratado desde 2022, servicios contratados mediante los expedientes de contratación C-37/2021 y C-32/2023, ambos financiados con Fondos Europeos del Mecanismos de Recuperación y Resiliencia (MRR). Para lograr los objetivos de esta prestación, actualmente en curso mediante el contrato C-32/2023, se ha analizado la situación de la seguridad en la ATM y diseñado un plan de mejora, que ha derivado en la planificación de actividades en diferentes ámbitos de actuación: operacional, de gestión y cumplimiento. Uno de los objetivos de este pliego es asegurar en la ATM la continuidad del servicio del CISO hasta la finalización de estas actividades, para realizar su seguimiento y garantizar que se desarrollen en los términos y objetivos establecidos, así como colaborar con la consolidación de un sistema suficientemente maduro de Sistema de Gestión de la Seguridad de la Información (SGSI) y que se cumpla el marco normativo que le corresponde a la ATM en ciberseguridad.

La ATM también ha empezado, mediante los contratos de los exp. C-27/2023 -relativo a los servicios de Adecuación al ENS- y el exp. C-28/202 -relativo a los servicios de Auditoría Continuidad y DRP-, tareas para adecuarse a la normativa ENS y revisar sus planes de continuidad. De cara a poder dar continuidad a los servicios prestados en la ejecución de estos contratos, hace falta reforzar la figura del CISO con un rol experto en gobernanza, gestión del riesgo y cumplimiento -el acrónimo GRC en adelante-, para asegurar que la organización funciona de manera segura, controlada y alineada con las leyes y normas, los riesgos y los objetivos estratégicos, apoyando en las operaciones del rol CISO.

Este PPT también contempla la prestación de los servicios 24x7x365 para realizar funciones operacionales del Sistema de monitorización, Gestión de acontecimientos, Información de seguridad y también servicios propios de un SOC (*security operations center*) con capacidad de respuesta (CSIRT), principalmente como servicio de gestión y configuración de seguridad, así como de respuesta ante incidentes.

En el presente Pliego de Prescripciones Técnicas se describen las necesidades al respecto.

En consonancia con el principio básico de "Líneas de defensa" establecido en el Real Decreto 311/2022 del 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad (ENS), que aplicado a la Administración Pública y en concreto a la ATM, tiene como objetivo orientar la estrategia de seguridad hacia una solución de garantía de protección adecuada de la información y los servicios que gestiona el ente y los proveedores que trabajan en él, para garantizar la seguridad de la información, los sistemas y los servicios electrónicos, asegurando que funcionen de manera segura, fiable y resiliente.

3. Objeto del contrato

El objeto del contrato es la externalización del servicio CISO, con el fin de proteger la organización definiendo la estrategia de ciberseguridad, gestionando riesgos, garantizando el cumplimiento normativo, monitorizando los sistemas de información de la ATM contra accesos no autorizados, y liderando la respuesta ante incidentes, con visión transversal y alineación con el negocio, de forma que impida comprometer la confidencialidad, integridad y disponibilidad de los datos que son almacenados, procesados y transmitidos.

El presente pliego tiene por objeto la prestación de un servicio de CISO, con la particularidad de garantizar la continuidad de las acciones iniciadas en el actual servicio de CISO (contrato en vigor, exp. C-32/2023). Por eso tendrá que monitorizar y coordinar la ejecución de las actividades promovidas desde el ámbito de Seguridad corporativa, para garantizar que su ejecución se realiza en los términos acordados. Este rol estará reforzado con un rol profesional experto en gobernanza, riesgo y cumplimiento (GRC), junto con un servicio de Security Operations Center (SOC).

Así, es necesario mantener la actual caracterización del servicio de externalización de CISO y reforzarla con un rol profesional de GRC (Governance, Risk & Compliance) que combine visión estratégica, comprensión normativa, capacidad técnica y habilidades de gestión. Asegurar la continuidad de la correcta ejecución de las actividades iniciadas durante el actual contrato, identificar puntos de mejora continua en las mismas, aportar bases sólidas para la gestión de riesgos corporativos, controles internos, auditoría, marcos regulatorios, contratos, gestión legal del riesgo y políticas corporativas, son necesidades que cubrir. El contrato también da continuidad a los servicios implicados con el Sistema de monitorización, gestión de acontecimientos, información de seguridad, Servicio de gestión y configuración de seguridad y de respuesta ante incidentes y a las licitaciones “C-27/2023 - Adecuación a ENS” y “C-28/2023 - Auditoría Continuidad y DRP”.

Con esta licitación, el órgano de contratación también pretende cubrir las necesidades de monitorear los sistemas de información de la ATM contra accesos no autorizados, así como gestionar los incidentes (SOC) y la respuesta (CSIRT) que impida comprometer la confidencialidad, integridad y disponibilidad de los datos que son almacenados, procesados y transmitidos.

Por otro lado, se requiere un apoyo al servicio y tareas realizadas por la figura del CISO con un rol experto en Gobernanza, Riesgo y Cumplimiento (GRC) en el marco normativo que la ATM tiene que cumplir, que pueda apoyar en las operaciones del CISO.

Asimismo, es objeto de la presente licitación encaminar la ATM a la adecuación a la nueva Directiva europea de Ciberseguridad, NIS2, de seguridad y resiliencia, en su vertiente no únicamente tecnológica, que afecta procesos, gobernanza, cadena de suministro y responsabilidades de dirección.

4. Actividades y funciones de la empresa adjudicataria

La prestación regulada en este pliego tiene que ajustarse, al menos, a los requisitos técnicos especificados en este pliego, sin perjuicio de los parámetros que se tienen que valorar mediante los criterios de adjudicación establecidos.

La empresa contratista tiene que disponer de los suficientes medios técnicos, materiales cualitativos y personales para desarrollar las tareas objeto del correspondiente contrato.

La prestación del servicio tendrá que cumplir con los parámetros de calidad y seguridad establecidos por la ATM, la legislación vigente y las principales normas y buenas prácticas aplicables a las tecnologías de la información y la comunicación, para garantizar la confidencialidad, disponibilidad e integridad de la información a la que pueda tener acceso la empresa adjudicataria en virtud del contrato.

Durante la prestación del servicio, la empresa adjudicataria, juntamente con la ATM, definirán las medidas técnicas y de gobernanza de seguridad más apropiadas para el servicio, de acuerdo con el análisis de riesgos que se lleve a cabo a tal efecto, en caso de que así se requiera.

La oferta que presente la empresa licitadora tendrá que alcanzar la totalidad de la prestación de servicios y realización de las tareas especificadas en el presente pliego y en el Pliego de Cláusulas Administrativas Particulares, siendo todas ellas obligatorias para la admisión de las propuestas.

Las funciones que tendrá que realizar la empresa adjudicataria son las siguientes.

4.1 Rol de CISO externalizado

El CISO es la figura que protege la organización definiendo la estrategia de ciberseguridad, gestionando riesgos, garantizando el cumplimiento y liderando la respuesta a incidentes, con visión transversal y alineación con el negocio.

En este apartado se establecen las tareas y responsabilidades de forma enunciativa, que no exhaustiva, de la empresa contratista adjudicataria, que incluyen las propias de un servicio de CISO externalizado:

- Alinear y dirigir la Ciberseguridad de la ATM con los marcos normativos que correspondan, comprendiendo la misión y los objetivos de la ATM y asegurar que las actividades se planifican y ejecutan.

- Diseñar la continuación de la estrategia global de seguridad alineada con el negocio, minimizando cualquier gap.

- Satisfacer estos objetivos garantizando la continuidad y resiliencia en el plan de seguridad y su hoja de ruta.

- Recabar una visión de negocio que comprenda los riesgos que afronta la organización, su gestión y el plan de continuidad y auditoría.

- Establecer políticas y marcos donde la ATM es responsable de adecuación y cumplimiento (ISO, NIST, ENS, NIS, Zero Trust...).

- Dirigir el programa de gestión de riesgos de la organización y la cadena de suministro y proveedores.

- Diseñar y dirigir la protección de la información y gestión de vulnerabilidades

- Gestión del SOC y respuesta a incidentes

- Cultura y concienciación en Ciberseguridad. Formación, buenas prácticas y sensibilización.

- Revisar arquitectura técnica y de comunicaciones en proyectos

- Supervisar las infraestructuras de sistemas y la administración del control de acceso a la información.

- Integrar seguridad en el ciclo de vida del software (DevSecOps).

- Validar planes de gestión de crisis, continuidad y resiliencia.

- Informar a la dirección sobre riesgos, incidentes y estado de la seguridad en la ATM.

4.2 Rol de experto en Gobernanza, Riesgo y Cumplimiento (GRC)

El rol principal de un GRC es garantizar que la organización es segura, cumple la normativa y gestiona sus riesgos de forma proactiva y ordenada.

En este apartado se establecen las tareas y responsabilidades de forma enunciativa, que no exhaustiva, de la empresa contratista adjudicataria, que incluyen las propias de un experto en GRC:

- Asesorar al CISO y la ATM en materia de normativas.
- Asegurar que la organización opera de forma coherente con su estrategia.
- Coordinar áreas y asegurar que todos siguen las mismas reglas.
- Detectar riesgos operativos, tecnológicos, legales de ciberseguridad.
- Evaluar el impacto y probabilidad.
- Organizar y asegurar el cumplimiento de normativas aplicables (GDPR, ENS, NIS2, ISO, directrices del CCN...).
- Gestionar auditorías internas y externas.
- Definir controles, pruebas y evidencias.
- Apoyar al CISO en la propuesta de planes de mitigación y supervisar que se cumplan.
- Liderar el servicio de gestión y configuración de seguridad y respuesta ante incidentes, descrito en el punto 4.4 de este documento, en coordinación con el CISO.
- Apoyar al CISO en todo aquello que requiera en el marco de gestión de la seguridad, gestión de riesgos y cumplimiento.

4.3 Sistema de monitorización y gestión de acontecimientos e información de seguridad

La ATM dispone de un sistema de gestión de acontecimientos de información de seguridad (Security Information and Event Management), que referiremos como SIEM, que permite la monitorización y la correlación de acontecimientos de seguridad, integrando las fuentes de datos que generen todos los dispositivos y sistemas de red de la T-mobilitat, con el objetivo de detectar anomalías de seguridad y generar alertas que permitan la adecuada clasificación del nivel de amenaza de cualquiera de los incidentes de seguridad detectados.

La empresa contratista aprobará las automatizaciones y correlaciones a implantar en las herramientas de ciberseguridad de la ATM, detallando los casos de uso a implantar por la empresa suministradora de las herramientas a contratar (objeto de otra licitación) a la que deberá proporcionar, como mínimo cada 2 meses, los registros de actividad completos en formato interoperable para su análisis.

4.4 Servicio de gestión y configuración de seguridad y respuesta ante incidentes

Este servicio comprenderá la gestión de la supervisión de la instalación y configuración de todos los elementos de seguridad, así como la definición de las integraciones a proponer.

También comprenderá la dirección proactiva de todas las actualizaciones de hardware y software aplicables a todos los sistemas, de acuerdo con las especificaciones de las respectivas empresas fabricantes y suministradoras, así como, si corresponde, la dirección de las reconfiguraciones necesarias para adecuarse a la evolución de los sistemas existentes a lo largo del tiempo, en materia de seguridad.

La empresa contratista dispondrá de un centro de operaciones de seguridad (*security operations center*), en adelante SOC, con todas las capacidades necesarias para la prestación del servicio. El SOC tendrá que disponer de personal especializado en la gestión de la seguridad de la información e incidentes de seguridad, así como de gestión de la respuesta a los incidentes (CSIRT).

La prestación del servicio se realizará en régimen de 24x7x365 días y prioritariamente desde centros ubicados en la Unión Europea, cumpliendo todas las normas aplicables en vigor.

El servicio contemplará la clasificación y priorización de las alertas generadas por el SIEM y otros sistemas afines, el tratamiento de los incidentes de seguridad que no hayan sido contenidos mediante configuraciones preestablecidas en el sistema y la implantación de un modelo de mejora continua, según las amenazas y vulnerabilidades que pudieran ir sucediendo durante la duración del contrato.

Dentro de este servicio se contemplará la gestión de vulnerabilidades, tanto de la infraestructura (comprendiendo tanto los fallos de software como de la configuración) como de todas aquellas aplicaciones accesibles desde Internet, y las propuestas para la corrección de estas.

La empresa contratista asumirá también la coordinación para la activación de mecanismos de seguridad, no incluidos en este contrato, prestados por terceras partes para la ATM, en particular el servicio de acciones de monitorización y gestión de alertas y respuesta 24x7x365 (SIEM), no incluido en esta licitación. El SIEM está contratado con un tercero. La función de la empresa adjudicataria de esta licitación se reduce a la coordinación para la activación de mecanismos de seguridad, no a la prestación del SIEM.

Finalmente, el servicio contemplará la asistencia para la recogida *in situ* de evidencias forenses relativas a incidentes de seguridad y su custodia y preservación a efectos legales y/o procesales.

Se coordinará con la Agencia de Ciberseguridad de Cataluña y otros centros de referencia y respuesta ante incidentes y entidades de naturaleza similar dentro de la administración de la Generalitat de Cataluña y dentro del ámbito del ecosistema de influencia de la ATM: administraciones titulares (operadores de transporte, etc.).

La ATM dispone de su Política de Seguridad que articula la gestión continua de la seguridad y requiere de la organización, la implantación del proceso de seguridad y auditoría, alineando la seguridad de la información con los objetivos de cumplimiento normativo y de

negocio, para garantizar la continuidad de la actividad y la protección de la información en un marco de mejora continua.

La empresa contratista será la encargada de generar e implantar las políticas de seguridad de la información que correspondan; garantizar la seguridad y privacidad de los datos y dirigir y supervisar tanto la administración del control de acceso a la información como el cumplimiento normativo de la seguridad de la información vigente a lo largo del contrato. A tal efecto, el objetivo a lograr es el cumplimiento normativo y de operaciones en materia de seguridad por parte de la ATM.

En caso de que en un futuro se vuelva a licitar el objeto del presente contrato, expediente C-25/2025, la empresa adjudicataria deberá llevar a cabo el traspaso de conocimiento con un periodo mínimo de dos meses, durante los cuales el CISO saliente informará al CISO entrante de las infraestructuras de la ATM, así como de todas las acciones de ciberseguridad en curso o pendientes de ejecutar. Esta tarea de transferencia de conocimiento será planificada por el CISO saliente; la ejecución será responsabilidad de la nueva empresa adjudicataria, que informará semanalmente de su avance.

5 Finalidades y objetivos que lograr

Las finalidades que se logran mediante la realización de este contrato consisten en garantizar y consolidar la continuidad de las acciones ya iniciadas por el actual servicio de CISO, así como asegurar la correcta ejecución de nuevas necesidades surgidas a este respecto.

Con esta licitación, el órgano de contratación también pretende complementar las necesidades de monitorear los sistemas de información de la ATM contra los accesos no autorizados, así como gestionar los incidentes (SOC) y la respuesta (CSIRT) que impida comprometer la confidencialidad, integridad y disponibilidad de los datos almacenados, procesados y transmitidos.

De este modo, la ATM podrá seguir disponiendo de un CISO que pueda diseñar el marco requerido en la gestión de la ciberseguridad y protección de datos, coordinar la necesidad de aumentar las herramientas de ciberseguridad y su explotación, el control de los datos de las organizaciones, así como adaptar a las diferentes normativas como el Esquema Nacional de Seguridad, las políticas de gobierno de seguridad aplicables a la ATM como organización de sector público de la Generalitat de Cataluña o a estándares como ISO aplicables.

La empresa contratista será la encargada de generar e implantar las políticas de seguridad de la información; garantizar la seguridad y privacidad de los datos y dirigir y supervisar tanto la administración del control de acceso a la información, como el cumplimiento normativo de la seguridad de la información. A tal efecto, el objetivo a lograr es el cumplimiento normativo y de operaciones en materia de seguridad (ENS, NIS, toda la normativa aplicable) por parte de la ATM.

Además, es la responsable de dirigir el equipo de respuesta ante incidentes que se produzcan en el ámbito de Seguridad y estará al cargo de la arquitectura de seguridad de la información de la organización.

6 Requerimientos técnicos generales obligatorios de la prestación y/o rendimiento o exigencias funcionales de la prestación

La empresa contratista dispondrá de los suficientes medios técnicos, materiales cualitativos y personales para desarrollar las tareas objeto de este contrato.

Tareas básicas que realizar:

- Dirigir, orientar y coordinar la estrategia de seguridad, de control del riesgo, de recuperación y continuidad.
- Definir la normativa de seguridad y procurar que se cumpla.
- Prevenir, detectar y analizar vulnerabilidades.
- Establecer e implementar políticas y auditoría debidas relacionadas con la seguridad.
- Informar y reportar a dirección.
- Garantizar la seguridad en la privacidad de los datos de la ATM.
- Alinear la seguridad con la continuidad de negocio.
- Controlar y gestionar los recursos del servicio objeto del contrato.
- Diseñar programas de formación y concienciación a la ATM.

Requerimientos mínimos de equipo humano:

Perfil	Experiencia / Conocimientos
Rol de CISO externalizado	• **Titulación:** Mínimo grado en ingeniería informática, telecomunicaciones o equivalente • **Experiencia:** Mínimo 5 años de experiencia profesional en el ámbito de sistemas tecnológicos. Se valorará: • **Conocimientos:** es valorarán titulaciones, certificaciones y experiencia en el ámbito de la ciberseguridad.
Rol de experto en GRC	• **Titulación:** Mínimo ciclo formativo de grado superior o titulación de grado universitario del ámbito de informática y comunicaciones, derecho, administración y gestión o similares.

	• **Experiencia:** Mínimo 3 años de experiencia profesional en el ámbito de sistemas tecnológicos Se valorará: • **Conocimientos:** es valorará titulaciones, certificaciones y experiencia en el ámbito de la ciberseguridad y de gobierno, gestión de riesgos y cumplimiento.
Servicio 24x7x365	• Capacitación de conocimientos, experiencia, formación en seguridad de sistemas de la información y/o telecomunicaciones y certificación del servicio.

Más allá de los requisitos mínimos que tiene que cumplir el equipo humano, se valorará la experiencia tanto del perfil CISO, como del experto en GRC,

Tanto el perfil CISO, como el experto en GRC y el equipo asignado al servicio 24x7x365 (SOC) han de disponer de conocimientos legales del ámbito del objeto del contrato, concretamente en relación con la normativa relativa al cumplimiento del ENS, la NIS, así como experiencia en todos aquellos requisitos de servicio definidos.

Durante la vigencia del contrato, la ATM proporcionará las herramientas y los equipos informáticos y los accesos necesarios para la realización del trabajo del perfil servicios CISO y del perfil experto en GRC, dando por sentado que el resto de los recursos necesarios para la prestación de los servicios (SOC propio) serán proporcionados por la propia empresa contratista.

Las personas designadas para ejercer los perfiles de CISO y de GRC dispondrán de teléfono móvil de contacto. La ATM no proporcionará el teléfono móvil, ni el servicio de telefonía, ni datos asociados al citado dispositivo. Tampoco asumirá ningún gasto de conectividad en el marco de trabajo fuera de las oficinas de la ATM en términos amplios dentro de la prestación del servicio contractual de referencia.

El equipo mínimo que la empresa pone a disposición del proyecto se tiene que mantener a lo largo de la vigencia del contrato. Excepcionalmente, en caso de que fuera necesaria la sustitución del CISO o del GRC, la ATM tendrá que aceptar previamente esta sustitución, validando que el nuevo perfil cumple el mismo nivel de solvencia técnica o superior, y que tendrá que estar operativo en un máximo de tres semanas.

En este orden de cosas, se hace constar que la ATM queda desvinculada, a todos los efectos, de cualquier relación laboral con el personal de la entidad adjudicataria, dado que se trata de un contrato de apoyo y asistencia que tiene que ser considerado como tal en su conjunto.

7 Formas de seguimiento y control de la ejecución de las condiciones

El órgano de contratación designará una persona que asumirá el control y la coordinación de la ejecución contractual con la empresa adjudicataria para tratar directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego.

La empresa adjudicataria designará como interlocutor único con la ATM al perfil que ejercerá las funciones del CISO como persona responsable a quien encargar la gestión de la ejecución del contrato y que tendrá que garantizar la calidad de la prestación objeto de este pliego, tratando directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego con la persona interlocutora designada por el órgano de Contratación.

En la fase inicial se analizará el modelo de Sistema de Gestión de la Seguridad de la Información establecido, así como su grado de madurez y el grado de cumplimiento de su marco normativo.

En la siguiente fase se analizará el estado de las actividades en curso, con especial cuidado con la identificación de riesgos de ejecución, finalización, etc.

La dirección de los controles organizativos incluirá la coordinación de todos los agentes, internos y externos a la ATM que tengan relación con la seguridad y ciberseguridad, asignación de responsabilidades, políticas y supervisión, estructuración de los procedimientos de información, etc.

Con periodicidad mensual, la empresa contratista elaborará un informe de seguimiento, identificando las actividades, el ciclo de resolución de los incidentes de seguridad, clasificados por tipologías y nivel de gravedad, de forma genérica, pero abiertos a adecuarlo con la información que en su momento sea requerida por la ATM.

Además de con la ATM, en nombre de quien ejercerá su rol, el CISO se coordinará estrechamente con la Agencia Catalana de Ciberseguridad (ACC) y el CTTI de la Generalitat de Cataluña y cualquier otro ente de orden superior a la ATM que en materia de Ciberseguridad sea preceptivo y/o necesario.

La disponibilidad de la empresa contratista es 24x7x365 para atender cualquier incidente y liderar el escalado de responsabilidad, a pesar de que la jornada de desarrollo de su rol se enmarca en el horario de las oficinas de la ATM.

En todo momento, la empresa contratista estará sujeta y ejercerá el servicio objete de esta contratación teniendo en cuenta la perspectiva medioambiental, social, laboral y de innovación que proceda, en el marco de las funciones de este contrato.

Para el CISO y el experto GRC la ejecución del contrato se llevará a cabo en las dependencias, calendario laboral y horario de la ATM. Las jornadas laborales se ejecutarán de forma presencial y en teletrabajo, según las normas de la ATM y de los requerimientos necesarios que disponga la ATM. El desarrollo de las tareas del SOCO no se realizará desde dependencias de la ATM.

La empresa adjudicataria tendrá que facilitar, en tiempo y forma, la información que le sea requerida para acreditar el cumplimiento de los objetivos fijados. La carencia de entrega de

esta información o su entrega incompleta, fuera de plazo o sin respetar las especificaciones de este pliego y resto de prescripciones técnicas del contrato, podrá ser considerada causa de incumplimiento.

8 Calendario de trabajo y duración del Contrato

Se establece una duración del presente contrato de un año, con posibilidad de dos prórrogas por un plazo de un año cada prórroga.

Dentro de los 10 días siguientes a la fecha de inicio de la prestación del objeto del contrato, la empresa contratista tendrá que librar al director responsable del contrato el programa de trabajo para su aceptación. La dirección del contrato resolverá sobre el programa de trabajo dentro de un plazo de 5 días contados a partir de la fecha de entrega, entendiendo que la resolución podrá introducir modificaciones, siempre que no contravengan las condiciones del contrato.

Tal como se ha definido en el punto 4, además de los aspectos relacionados con los requerimientos técnicos generales obligatorios de la prestación y/o rendimiento o exigencias funcionales de la prestación, la empresa adjudicataria se responsabilizará de tareas de gestión, mejoras, ajustes y aspectos de mantenimiento que puedan surgir, hasta la fecha final de ejecución del contrato.

Durante la ejecución del contrato, la empresa adjudicataria tendrá que facilitar a la dirección del contrato por parte de ATM cualquier información solicitada con un plazo máximo de entrega de 5 días hábiles.

9 Condiciones generales de ejecución y ciberseguridad

9.1 Principios básicos

- **Deber de confidencialidad.** El personal de la empresa adjudicataria tiene que mantener absoluta confidencialidad y estricto secreto sobre la información conocida a raíz de la ejecución de los servicios contratados. Esta obligación de confidencialidad tiene carácter indefinido y subsistirá incluso después de haber cesado su relación laboral con la ATM. La empresa adjudicataria tiene que comunicar esta obligación de confidencialidad a su personal y tiene que controlar su cumplimiento. La empresa adjudicataria tiene que poner en conocimiento de la ATM, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar la integridad o la confidencialidad de la información. Este deber se extiende al personal de otras empresas que, a petición de la empresa adjudicataria, participen en la prestación de los servicios recogidos en este pliego.

- **Propiedad intelectual**: Toda la documentación que se genere durante la prestación de los servicios de apoyo es propiedad exclusiva de la ATM.

  Toda la documentación generada en la presente contratación será propiedad de la ATM y no se podrá hacer ningún uso por parte de la empresa adjudicataria, así como todos los desarrollos realizados dentro de la presente licitación.

- **Criterios de accesibilidad universal:** La empresa adjudicataria se responsabilizará de cumplir con los criterios de accesibilidad universal, tal como están definidos en el texto refundido de la Ley General de derechos de las personas con discapacidad y de inclusión social, aprobado rmediante Real decreto legislativo 1/2013, de 29 de noviembre.

  Los medios de comunicación, el diseño de los elementos instrumentales y la implantación de los trámites procedimentales empleados por la empresa contratista en la ejecución del contrato tendrán que realizarse teniendo en cuenta los criterios de accesibilidad universal y de diseño para todo el mundo.

- **Criterios de sostenibilidad y protección al medio ambiente:** La empresa adjudicataria se responsabilizará de cumplir los criterios de sostenibilidad y protección del medio ambiente, de acuerdo con las definiciones y principios regulados en los artículos 3 y 4, respectivamente, del *Real decreto legislativo 1/2016, de 16 de diciembre, por el cual se aprueba el texto refundido de la Ley de prevención y control integrados de la contaminación*.

  Siempre que sea posible, la empresa contratista tendrá que hacer una elección inteligente de materiales (uso de materiales adecuados para el medio ambiente, evitando los que no lo sean), equipos de eficiencia energética (reducir el coste energético y la huella de carbono colectivo), final de la vida útil y reutilización, etc.

9.2 Marco de cumplimiento normativo

El actual marco normativo para las entidades públicas de Cataluña está establecido, principalmente, en la Política de Ciberseguridad de la Generalitat de Cataluña de septiembre del 2021. Esta política recoge directivas y reglamentos del Parlamento y Consejo Europeo, reales decretos del Estado español, así como instrucciones de la Generalitat de Cataluña. Este marco de cumplimiento normativo en temas de ciberseguridad y protección de datos alcanza a las entidades públicas de la Generalitat de Cataluña y a todos aquellos que participan en la prestación de sus servicios.

9.3 Datos de carácter personal

La empresa adjudicataria tratará los datos de carácter personal a los que acceda como consecuencia de la ejecución de este contrato, en conformidad con lo establecido en la normativa vigente en la materia.

La empresa adjudicataria se responsabilizará del uso adecuado de la información que se pueda obtener para proteger los datos personales, a lo largo de toda la fase de realización del objeto del contrato y también una vez finalizada, en base a las normativas internacionales sobre la materia y de cumplimiento obligado, entre ellos y expresamente, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de los datos mencionados, así como cualquier otra normativa nacional y de la Unión Europea que sea aplicable en materia de protección de datos y en relación con los datos personales a los que tiene acceso durante la vigencia de este contrato.

El incumplimiento de estas obligaciones constituye la infracción tipificada en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, sin perjuicio de las responsabilidades exigidas ante la jurisdicción ordinaria.

La empresa adjudicataria, con relación a aquellos datos que por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) sea necesario, hay de cumplir en la solución propuesta, por ejemplo, ubicar los datos en una base de datos física diferente, cifrar los datos, control de acceso, etc.

La empresa adjudicataria se compromete a cumplir, con relación a los datos tratados en la ejecución del presente contrato:

- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Las buenas prácticas para la gestión de la seguridad de la información.

9.4 Esquema Nacional de Seguridad (ENS)

El artículo 2 del vigente Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad, dispone que los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación del real decreto del ENS contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el mismo de los sistemas de información en los cuales se sustenten los servicios prestados por las empresas contratistas, como por ejemplo la presentación de las correspondientes Declaraciones o Certificaciones en conformidad con el ENS. Esta cautela se extenderá también a la cadena de suministro de estas empresas contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

La ATM considera necesario que las empresas proveedoras que vayan a concurrir a esta licitación tendrán que estar en condiciones de exhibir la correspondiente Declaración o Certificación en conformidad con el ENS. Así pues, en base a lo

anterior, y en el análisis de los riesgos a los cuales están expuestos los servicios objeto de la licitación, la ATM establece como necesario que las entidades licitadoras tendrán que estar en condiciones de exhibir la correspondiente Declaración en conformidad con el Esquema Nacional de Seguridad, para la categoría de seguridad BÁSICA, o superior, de los sistemas que intervengan en la prestación de los servicios indicados, así como mantener la conformidad en vigor durante la vigencia del contrato. Esta declaración o certificado en conformidad con el ENS tiene que alcanzar el ámbito objeto de la contratación.

En el supuesto de que la empresa adjudicataria no pudiera mantener la conformidad con el ENS durante la vigencia del contrato - por imposibilidad de mantener la Declaración de Conformidad o pérdida, retirada o suspensión de la Certificación de Conformidad -, tendrá que comunicar esta circunstancia, de manera inmediata y sin más dilación indebida, a la ATM, quien considerará el impacto de esta circunstancia en la prestación objeto del contrato.

Se establece un mecanismo provisional de acreditación de cumplimiento con el ENS, que consiste con la posibilidad de las empresas proveedoras de presentar informes de auditoría, declaraciones de aplicabilidad o procesos de certificación en curso; la aceptación de estos documentos dependerá de la validación por parte de la ATM. Se establece la asignación de la empresa adjudicataria, como fecha tope para la entrega de la Declaración o Certificados de Conformidad del ENS.

Se valorará un mayor nivel del cumplimiento del ENS por encima del mínimo requerido.

Los requerimientos de este marco de cumplimiento normativo no excluyen otros requerimientos de ciberseguridad que puedan estar incluidos en este pliego.

La documentación que entregará la empresa adjudicataria incluye el Plan de seguridad. Uno de los aspectos fundamentales a incluir en este documento es el modelo de gestión que se realizará en las fases de diseño e implantación, para asegurar la conformidad de la plataforma, con el marco de cumplimiento normativo, en la fase de explotación.

9.5 Seguimiento

La empresa adjudicataria asignará una persona responsable de seguridad y protección de datos para tratar los temas de ciberseguridad. La empresa adjudicataria incluirá en la hoja de ruta de seguridad un modelo de seguimiento de la ciberseguridad en función de la fase del proyecto.

10 Documentación técnica que tienen que aportar las empresas licitadoras

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta serán condiciones de cumplimiento obligado a lo largo de la ejecución del contrato, si esta es la adjudicataria.

La propuesta técnica tendrá que incluir una descripción de la metodología de trabajo, de los servicios a prestar, que tendrá que incluir también el apoyo del SOC 24x7, teniendo en cuenta la sistemática que utilizará para llevar a cabo la prestación con las especificidades particulares que garanticen su correcta ejecución e interrelación con la ATM.

Incluirá también la titulación adicional y experiencia de los perfiles CISO y GRC a adscribir a la ejecución del contrato.

Joaquim Colomé Batlle
Jefe de Unidad del Área de Sistemas e innovación

Firmado electrónicamente